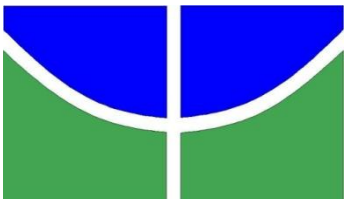


Universidade de Brasília

Instituto de Ciências Exatas

Departamento de Ciência da Computação

ASSINATURA DIGITAL EM CHEQUES BANCÁRIOS COM BASE NO PROCESSAMENTO DE IMAGENS

Aloísio de Ávila Dourado

Monografia apresentada como requisito parcial para
conclusão da graduação em Engenharia de Computação

Orientador

Prof. Dr. Bruno Luigi Machiavelo Espinoza

Brasília - DF

2015

Universidade de Brasília – UnB
Instituto de Ciências Exatas
Departamento de Ciência da Computação
Graduação em Engenharia de Computação

Coordenador: Prof. Dr. Ricardo Zelenovsky

Banca examinadora composta por:

Prof. Dr. Bruno Luiggi Macchiavello (Orientador) – CIC/UnB

Prof. Dr. Flávio de Barros Vidal – CIC/UnB

Prof. Dr. Alexandre Zaghetto – CIC/UnB

CIP – Catalogação Internacional na Publicação

Dourado, Aloísio de Ávila.

Assinatura Digital em Cheques Bancários com Base no Processamento de Imagens / Aloísio de Ávila Dourado. Brasília : UnB 2015.

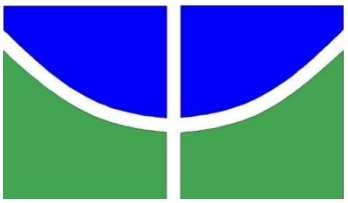
68 p. : il. ; 29,5 cm.

Monografia (Graduação) – Universidade de Brasília, Brasília, 2015.

1. cheque, 2. processamento de imagens, 3. assinatura digital, 4. marca d'água, 5. segurança.

CDU 004

Endereço: Universidade de Brasília
Campos Universitário Darcy Ribeiro - Asa Norte
CEP 70910-900
Brasília-DF – Brasil



Universidade de Brasília

Instituto de Ciências Exatas

Departamento de Ciência da Computação

ASSINATURA DIGITAL EM CHEQUES BANCÁRIOS COM BASE NO PROCESSAMENTO DE IMAGENS

Aloísio de Ávila Dourado

Monografia apresentada como requisito parcial para
conclusão da graduação em Engenharia de Computação

Prof. Dr. Bruno Luigi Machiavelo Espinoza (Orientador)
CIC/UnB

Prof. Dr. Flávio de Barros Vidal
CIC/UnB

Prof. Dr. Alexandre Zaghetto
CIC/UnB

Prof. Dr. Ricardo Zelenovsky
Coordenador do Curso de Engenharia de Computação

Brasília, 10 de Dezembro de 2015

RESUMO

Cheques bancários são uma importante ferramenta de transferência de recursos financeiros, portanto é necessário que sua segurança seja reforçada. Este trabalho tem como objetivo desenvolver uma técnica de assinatura digital, por meio de marca d'água, para incrementar a segurança dos cheques contra reprodução indevida. Para isso foram utilizados conceitos e ferramentas de processamento de imagens em conjunto com técnicas de *hashing*. Durante o processo de pesquisa foi possível desenvolver uma técnica de assinatura digital capaz de inserir uma marca d'água imperceptível ao olho humano na imagem do cheque. Essa técnica foi capaz de recuperar a assinatura inserida com acerto de 100% em algumas baterias de testes realizadas, nas quais foram utilizadas folha de cheque em circulação do Banco do Brasil. Espera-se que o realizado possa ajudar na detecção de fraudes com cheques bancários, aumentando a segurança para bancos, clientes e lojistas.

Palavras-chave: cheque, processamento de imagens, assinatura digital, marca d'água, segurança.

ABSTRACT

Bank checks still are an important financial resource transfer tool that needs to have its security enhanced. This work aims to develop a digital signature technique by watermark, to increase the security of checks against unauthorized reproduction. Concepts and tools of image processing were used together with hashing techniques. It was possible to develop a digital signature technique able to insert a watermark imperceptible to the human eye in the image of the check. The technique developed was able to recover the signature inserted with 100% accuracy on some of our tests using the check sheet from "Banco do Brasil". We hope that this work can help to detect frauds to bank checks, increasing security for banks, costumers and shopkeepers.

Keywords: bank check, image processing, digital signature, watermark, security.

SUMÁRIO

Lista de Figuras

Lista de Tabelas

Lista de Abreviaturas, Siglas e Símbolos

Ad – Alteração detectada

Ae – Alteração esperada em %

BACEN – Banco Central do Brasil

BDR – Bloco *Dither Reverso*

BV – Bloco de Verificação

CAD – Contador Alterações Detectadas

Dpi – *Dots Per Inch*

ITI – Instituto Nacional de Tecnologia da Informação

MB – *Mega Bytes*

MBD – Média do Bloco Modelo

MBT – Média do Bloco Motivo

MD2 – *Message Digest 2*

MD4 – *Message Digest 4*

MD5 – *Message Digest 5*

RGB – *Red, Green and Blue*

TA – Taxa de Aceitação em %

Capítulo 1

Introdução

Apesar da crescente utilização de meios de pagamentos mais atuais, como a inserção de cartões magnéticos no mercado, o número de cheques compensados no Brasil ainda é muito relevante. Segundo pesquisa [1], entre janeiro e agosto de 2010, 747.539.896 cheques foram compensados. Ainda de acordo com a mesma fonte, esse número representa uma redução em relação a períodos anteriores, porém o valor dessas transações via cheque vem aumentando.

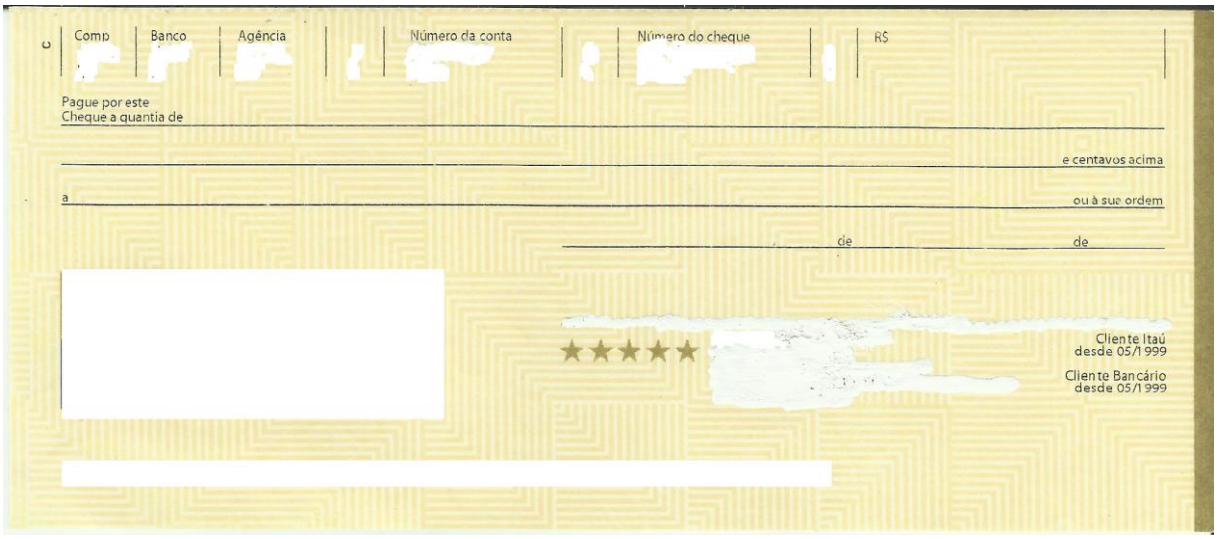
1.1 Descrição do Problema

O sistema brasileiro de compensação de cheques é regulamentado pelo BACEN (Banco Central do Brasil). A regulamentação atual [2] determina que a compensação de cheques seja efetuada unicamente por intermédio de imagem digital e outros registros eletrônicos do cheque, como a truncagem de cheques. A truncagem de cheques é um mecanismo de troca de cheques entre bancos por meio eletrônico, em substituição a troca física que ocorria anteriormente. Em [3], Dias apresenta um método para aumentar a segurança no processo de truncagem de cheques.

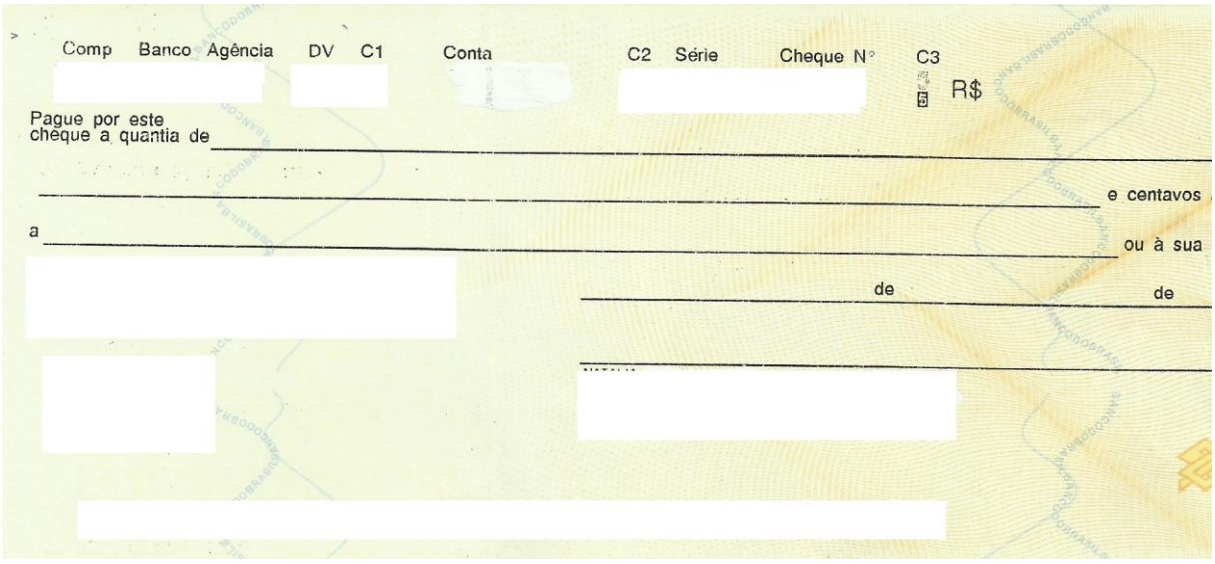
O acompanhamento manual da compensação de cheques somente ocorre em casos específicos, como quando existe indício prévio de fraudes, ou em casos de cheques de valores acima de determinada faixa. Devido ao alto número de cheques compensados diariamente no Brasil e a regulação do BACEN [2], que exige que os cheques de modo geral sejam compensados em até dois dias úteis, não é viável realizar a conferência manual de todos os cheques, sendo que em alguns casos apenas o valor do cheque é conferido de forma prática.

Nos demais, a compensação é feita de forma automática pelo sistema, sem conferência humana da assinatura do cheque.

Os bancos com atuação no Brasil elaboram as suas folhas de cheque seguindo algumas diretrizes constantes na resolução nº 3.972, de 28 de Abril de 2011 do BACEN [4]. Apesar disso, as folhas de cheques não são iguais entre os bancos, variando principalmente a imagem de fundo deles.



(a)



(b)

Figura 1.1: Exemplos de folhas de cheque brasileiros. (a) Folha de cheque do banco Itaú. (b) Folha de cheque do Banco do Brasil.

Existe uma grande preocupação com segurança quando tratamos de recursos financeiros, seja em seu armazenamento ou transferência. Alguns dos mecanismos de segurança que são utilizados atualmente pelos bancos são: certificados digitais e módulos de segurança acoplados aos sites bancários; senhas para validar a identidade do usuário no uso de cartões de crédito e débito; e marca d'água impressa nas cédulas de dinheiro para garantir sua autenticidade.

1.2 Objetivos do Trabalho

O objetivo desse trabalho é desenvolver uma técnica de assinatura digital que aumente a segurança na utilização do cheque. Pretende-se inserir nele uma marca d'água, de forma similar ao exemplo da cédula de dinheiro. Essa marca deve ser diferente para cada cheque impresso, variando de acordo com o número nele impresso e os dados do cliente.

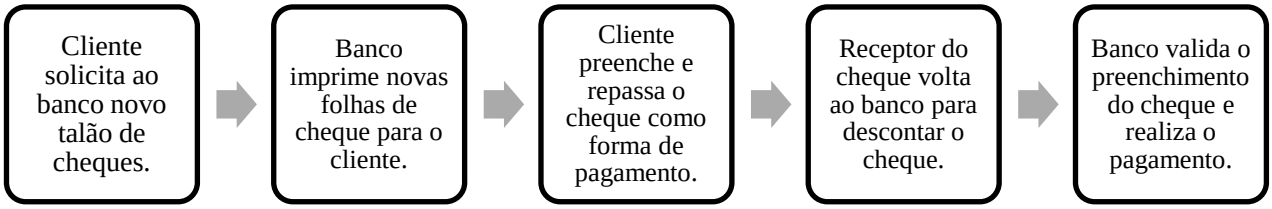


Figura 1.2: Fluxograma demonstrando as etapas atuais entre a impressão do cheque e a devolução do mesmo ao banco.

A assinatura inserida em forma de marca d'água deve ser imperceptível para o cliente bancário, assim apenas o sistema de validação do banco deve ser capaz de reconhecer a assinatura contida no cheque. Esse requisito foi criado para que a assinatura possa ser inserida no mercado de forma transparente para o cliente, sem causar estranheza; além disso, tal técnica aumentaria a segurança do cheque contra reproduções indevidas, que é uma questão de preocupação para os bancos [5].

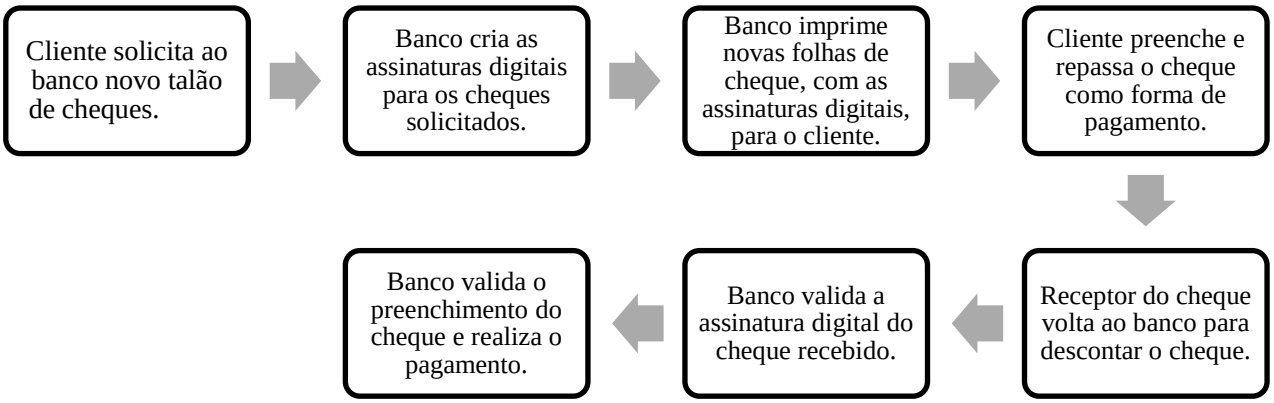


Figura 1.3: Fluxograma demonstrando as etapas do novo modelo proposto, entre a impressão do cheque e a devolução do mesmo ao banco.

Baseando-se nessas considerações, o presente trabalho será estruturado de maneira que no Capítulo 02 será apresentada uma introdução de conceitos relevantes para o entendimento da pesquisa. Em seguida, o Capítulo 03 será descrito o desenvolvimento da técnica proposta, com as equações utilizadas e descrição da metodologia. Os resultados obtidos vão ser apresentados e discutidos no Capítulo 04, levando à conclusão do trabalho no Capítulo 05. Por fim, as tabelas completas dos resultados podem ser encontradas no Apêndice.

Capítulo 2

Fundamentação Teórica

Nesse capítulo serão apresentados os principais conceitos da área de processamento de imagens, os quais são necessários para compreender o trabalho desenvolvido. Serão explicitadas características gerais de: Imagem digital; Entropia; Assinatura digital; *Hashing*; *Dithering;* e Marca d'água.

2.1 Imagem Digital

Gonzalez [6] define a imagem como uma função bidimensional *f (x, y),* em que *x* e *y* representam o espaço da imagem e o valor de *f*, em uma coordenada *(x, y)*, representa o nível de brilho daquele ponto. Quando os valores possíveis de *x*, *y* e *f* são finitos, pode-se representar essa imagem digitalmente. Este processo é obtido amostrando a imagem espacialmente e quantizando os valores de brilho.

Os elementos básicos da imagem digital são os pontos da função *f*, chamado de *pixels*. Como os *pixels* de uma imagem digital são finitos, é possível organiza-los em formato de matriz. Dessa forma, as imagens digitais são representadas como matrizes de dimensões *x* e *y*.

Essa representação permite que se façam operações algébricas no formato de matriz, que representa uma imagem digital, e obter como resultado outra imagem digital.

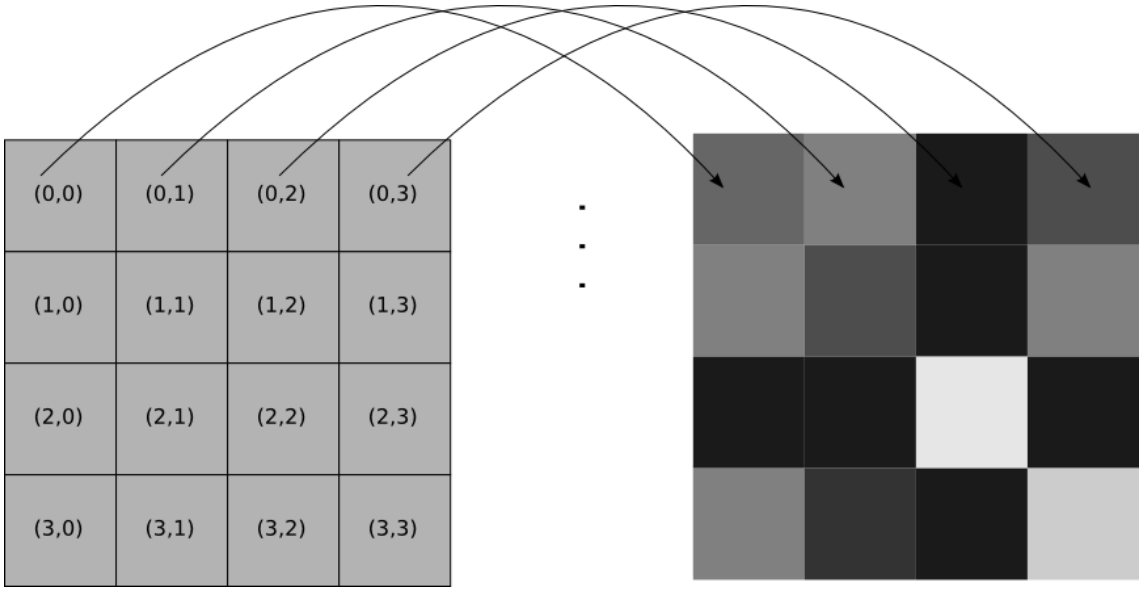


Figura 2.1: Exemplo de imagem e sua representação em formato de matriz.

A imagem digital definida anteriormente como uma função *f (x, y)* representa estritamente uma imagem monocromática (tons de cinza). Para imagens coloridas, utiliza-se uma função *f (x, y, z)*, em que *x* e *y* representam o espaço da imagem, e *z* representa um determinado canal de informação cromática. Um dos espaços de cores mais utilizados possui três canais: vermelho, verde e azul, ou em inglês *Red*, *Green*, *Blue* (RGB). A imagem passa, então, a ser representada como uma matriz de três dimensões, sendo que cada *pixel* dessa imagem possui três componentes de cores.

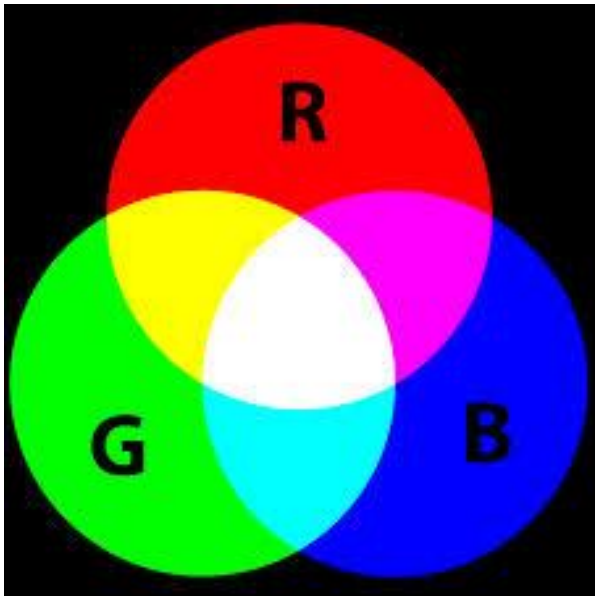


Figura 2.2: Espaço de cores RGB.

O sistema RGB é muito utilizado na representação da imagem digital colorida, pois consegue simular o espectro de cores perceptíveis pelo olho humano, utilizando para tal a soma de três cores básicas aditivas, o vermelho, o verde e o azul.

2.2 Entropia e redundância de uma imagem

Shannon [7], definiu a entropia H como o nível de incerteza de determinado conjunto de eventos aleatórios. Sendo *Pi* a probabilidade de cada um desses eventos, com *i* variando de *0* até *Imax*, temos:

$$H = -\sum_{i=0}^{Imax} Pi \, log_2 \, Pi \tag{2.1}$$

Pode-se considerar uma imagem digital como o resultado de um processo aleatório, no qual a probabilidade *Pi* corresponde à probabilidade de cada *pixel* da imagem possuir o valor de intensidade *i*. Desse modo, o conceito de *entropia* pode ser aplicado a imagens.

De acordo com Sanches [8], a compressão de uma imagem é possível por causa do alto grau de coerência dessa, que se traduz em redundância quando codificada. Essa redundância se reflete na alta probabilidade de *pixels* vizinhos de uma imagem possuírem valores semelhantes, por fazerem parte de um mesmo objeto desta, por exemplo.

No processo de compressão de imagens é necessário definir o número de *bits* utilizado para codificar cada nível de informação, a chamada *taxa de bits*. Essa taxa *B* varia de acordo com o número de níveis que é preciso codificar, de modo que se tem *N* níveis possíveis na codificação. Assim:

$$B = \log_2 N \tag{2.2}$$

O número *B* pode representar a taxa fixa, em caso de uma codificação uniforme, ou o número médio de *bits* utilizado, se for uma codificação não uniforme.

Pode-se, então, comparar a entropia da imagem com a *taxa de bits* para saber se esta é suficiente para representar a incerteza da imagem. Para que a compressão da imagem seja feita sem perdas, a *taxa de bits* deve ser maior ou igual à entropia da imagem.

2.3 Assinatura Digital

Assinar digitalmente um documento possui a mesma função de assinar um documento impresso: confirmar a autenticidade e integridade daquele. De forma semelhante ao que acontece no mundo físico com os cartórios, no mundo digital há agências e órgão certificadores de assinaturas, tal como o Instituto Nacional de Tecnologia da Informação (ITI) [9].

As assinaturas digitais se dividem em dois tipos básicos, assinatura simétrica e assinatura assimétrica. No primeiro tipo, existe apenas uma chave secreta, que deve ser conhecida pelo remetente da mensagem, para que ele possa assinar, e deve ser conhecida pelo destinatário, para que ele possa reconhecer a assinatura como verdadeira. O segundo tipo possui duas chaves, uma pública e outra privada, como explicado por Diffie e Hellman [10]. A chave privada serve para que o remetente assine a mensagem, enquanto que a chave pública é utilizada pelo destinatário para decodificar a assinatura e verificar sua autenticidade.

O método de assinatura proposto neste trabalho utiliza os conceitos de assinatura simétrica, com apenas uma chave privada. O principal ponto negativo desse método é a segurança no processo de divulgação da chave privada para as partes interessadas. Porém, no para o objeto de pesquisa em questão isso não é um problema, pois tanto o remetente, quanto o destinatário da mensagem são a mesma entidade, o sistema bancário.

2.4 Hashing

Oliveira [11] define uma função *hashing* como uma associação entre chaves e índices. Em uma função *hashing* ideal, cada índice estaria associado a uma única chave. Alterando a entrada *x* da função *Hashing H()*, mesmo que a alteração seja pequena, tem-se uma distorção considerável na saída *Y* da função.

$$Y = H(x) \tag{2.3}$$

Em um universo suficientemente grande, mesmo que a função *hashing* não seja ideal, é improvável que se tenha duas entradas com a mesma saída (colisão de *hashing*). De modo geral isso pode ser assim representado:

$$H(x1) \neq H(x2) \tag{2.4}$$

Nesse trabalho, o *hashing* foi utilizado no intuito de definir os pontos da imagem que seriam alterados para gerar a assinatura digital. O *Message Digest 5* (MD5) foi o tipo de *hashing* escolhido. O método MD5 foi inventado por Ron Rivest [12], sendo uma evolução mais segura do *Message Digest 4* (MD4) e *Message Digest 2* (MD2). Uma desvantagem do MD5 é o *hash* de saída com apenas 128 bits, porém para a aplicação dos cheques esse tamanho de saída é bastante satisfatório. Com N bits é possível endereçar 2^N endereços, portanto, uma vez que o número de pixels do cheque é muito menor do que 2^128, o tamanho da saída do MD5 é adequado para a aplicação.

O método de Rivest começa por normalizar a mensagem *M* de entrada. O tamanho da mensagem original é alterado adicionando um *bit '1'* e um número variável de *bits '0'*. Ao fim do processo a mensagem deverá ter um tamanho em *bits divisível por 512*, e terá nos *64 bits* finais a informação do tamanho original da mensagem, como pode ser constatado abaixo:

$$\textit{MENSAGEM ORIGINAL} + \textit{'1'} + \textit{'00...'} + \textit{Tamanho (mensagem original)} \tag{2.5}$$

Este processo inicial de normalização permite ao algoritmo aceitar entradas de tamanho fixo e apresentar uma saída de tamanho único. Após tal, a mensagem original é quebrada em mensagens de *512 bits*. Essas, por sua vez, são quebradas em 16 mensagens de *32 bits*. As mensagens de *32 bits* são combinadas em turnos, através de *operações bit a bit*. O final do processo gera um resultado de *128 bits*.

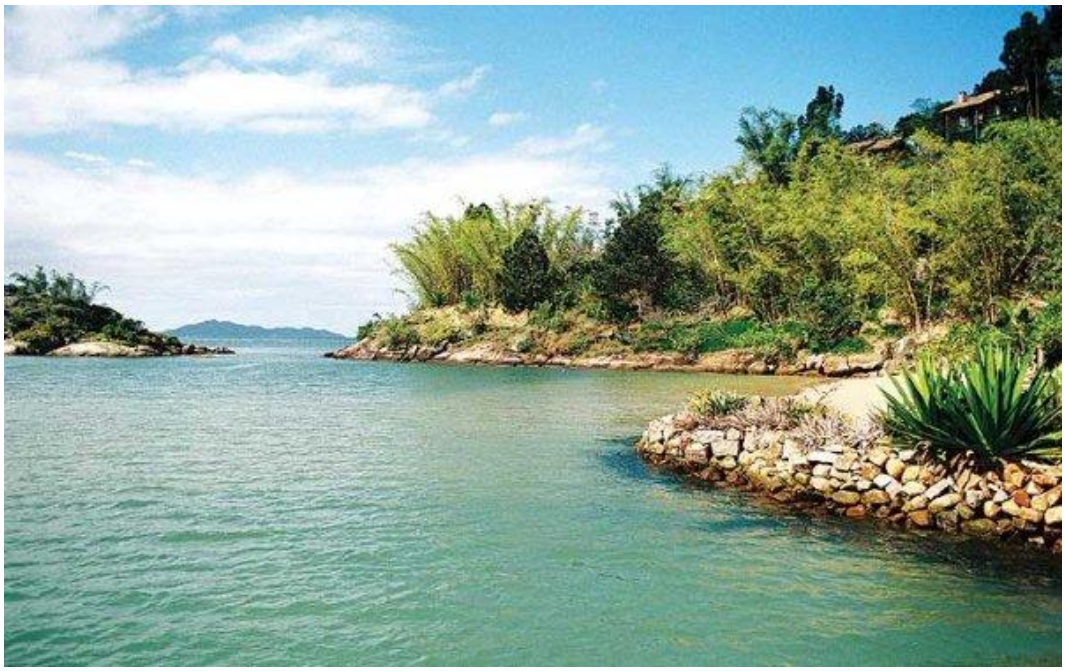
2.5 Dithering

Spencer [13] explica o método de *dithering* com propagação a de erros como uma maneira de mapear uma entrada no formato RGB em uma saída de uma tabela de cores previamente definida. Nesse método explicado cada *pixel* da imagem é analisado escolhendo para ele uma cor resultante pertencente à tabela de cores que mais se aproxime da sua

original. A tabela de cores usualmente não possui um espectro de cores tão amplo quanto o espectro utilizado na imagem original, por isso aproximações são feitas e erros são gerados.

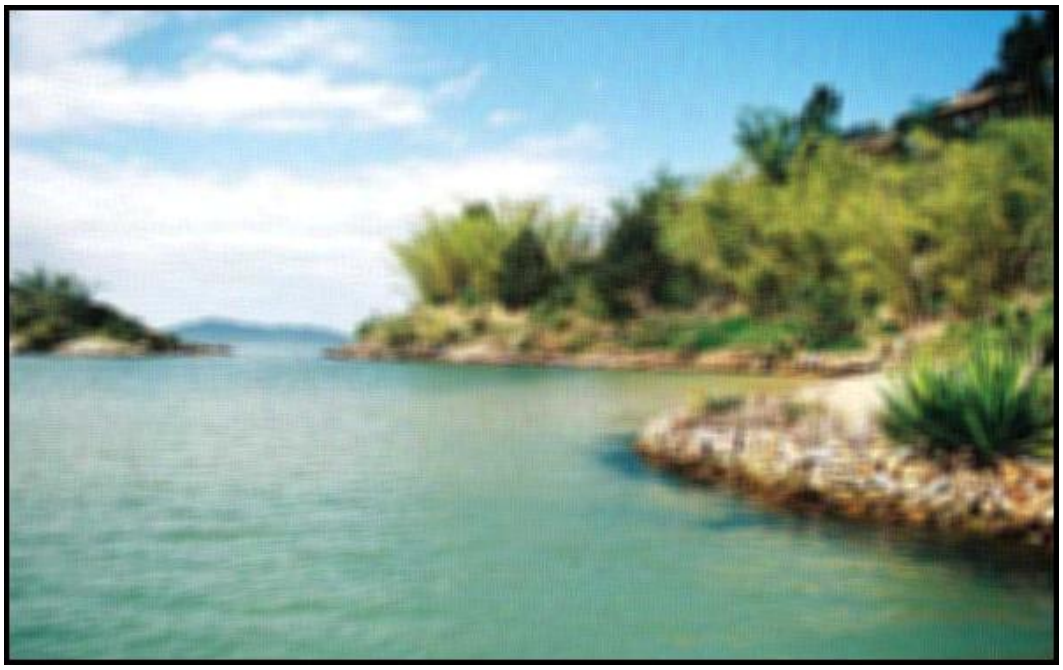
No processo de *dither*, calcula-se a diferença da cor escolhida para a cor real, chegando-se no erro de cada *pixel (Ep).* Esse erro é, então, diluído e espalhado para os *pixels* vizinhos, de forma a compensar o erro do *pixel* original. Se um *pixel* P(X,Y) possui *N pixels* vizinhos, então cada um desses *N vizinhos* possuem um erro *Ep(N)* associado e o algoritmo vai tentar compensar tais erros. Portanto, o valor que de fato será utilizado para o mapeamento na tabela de cores Vt(X,Y), do pixel P(X,Y) será:

$$Vt(X,Y) = P(X,Y) + \sum_{k=1}^{N} \frac{Ep(k)}{N} \quad (2.6)$$



(a)

(b)



(c)

Figura 2.3: Imagens do processo de Diher. (a) Imagem original. (b) Imagem após o processo de Dither. (c) Imagem após o processo de Dither Reverso.

Essa técnica será utilizada para simular a impressão dos cheques assinados digitalmente, acrescentando nas imagens processadas os ruídos que possivelmente serão incluídos pela impressora dos cheques.

O *dither reverso*, utilizado para desfazer o processo de *dither*, será utilizado para simular a digitalização dos cheques bancários.

No processo reverso, cada *pixel* da imagem deve ser analisado levando em conta seus vizinhos, para decodificar a propagação de erros mencionada no processo de *dither*. Dessa forma, é feita a média dos *pixels* em blocos, para determinar o valor do *pixel* central, transformando a imagem de volta para o formato RGB ao final do processo.

Todo o processo de *dither* seguido por *dither reverso* aplica alterações com perdas na imagem. Essas perdas podem ser significativas para a detecção da assinatura inserida na imagem.

2.6 Marca d'água

Watermark (marca d'água) é o nome que se dá à técnica de inserir informações em um documento, de maneira que essa informação só possa ser identificada sob condições específicas [14]. Um exemplo típico de documentos impressos com marca d'água são as cédulas de dinheiro, que possuem uma imagem de segurança, visível apenas quando olhada contra a luz.

Assinar um documento de maneira não visível ao olho humano não é um tipo de marca d'água. É desejável que se coloque bastante informação na assinatura, para aumentar sua segurança, mas, ao mesmo tempo, é necessário manter o nível de interferência na imagem muito baixo, para garantir sua discrição.

No trabalho de Brassil [15] foi desenvolvida uma técnica que insere informações em um documento alterando levemente a fonte do mesmo. Alterando o espaçamento entre as palavras de um documento, ele conseguiu de forma satisfatória inserir uma assinatura que garantisse a autenticidade de documentos impressos.

Mapear a técnica de Brassil para a assinatura dos cheques bancários não se mostrou viável, visto que os cheques não possuem muitos textos em que se pudesse inserir mudanças em seu espaçamento. A melhor saída para a assinatura do cheque seria alterar sua imagem de fundo.

Nguyen [16] mostrou em seu trabalho um método de assinatura que decompõe a imagem e depois assina a mesma levando em conta as principais características da visão humana (contraste e brilho).

Capítulo 3

Metodologia

Os procedimentos adotados para a assinatura digital dos cheques bancários serão descritos neste capítulo. Esses foram desenvolvidos ao longo do trabalho, e permaneceram os mesmo durante toda sua extensão, alterando-se apenas os parâmetros em busca de melhores resultados.

3.1 Estrutura geral

Nesse trabalho é proposto um sistema de assinatura digital de cheques com duas tarefas básicas: assinar digitalmente um cheque; e verificar a assinatura digital do cheque. O objetivo principal desse sistema é aumentar a segurança do processo vigente de emissão e pagamento de cheques.

No primeiro estágio do ciclo do cheque, ocorre a tarefa de assinatura. Nessa tarefa o sistema processa e mapeia a assinatura através da chave obtida via hashing, e em seguida insere a assinatura no cheque.

No segundo estágio o cheque assinado entra em circulação e é utilizado como pagamento pelo cliente. Eventualmente o cheque retorna ao banco nas mãos de um terceiro que deseja receber o recurso financeiro equivalente aquele cheque.

No terceiro estágio, quando o cheque retorna ao banco, ocorre a tarefa de verificação de assinatura. Nessa tarefa o sistema refaz o processamento da assinatura com a mesma chave obtida via hashing. O sistema então compara a assinatura processada com a assinatura obtida no cheque, e determina se o cheque é verdadeiro ou falso com base em parâmetros de aceitação definidos pelo administrador do sistema.

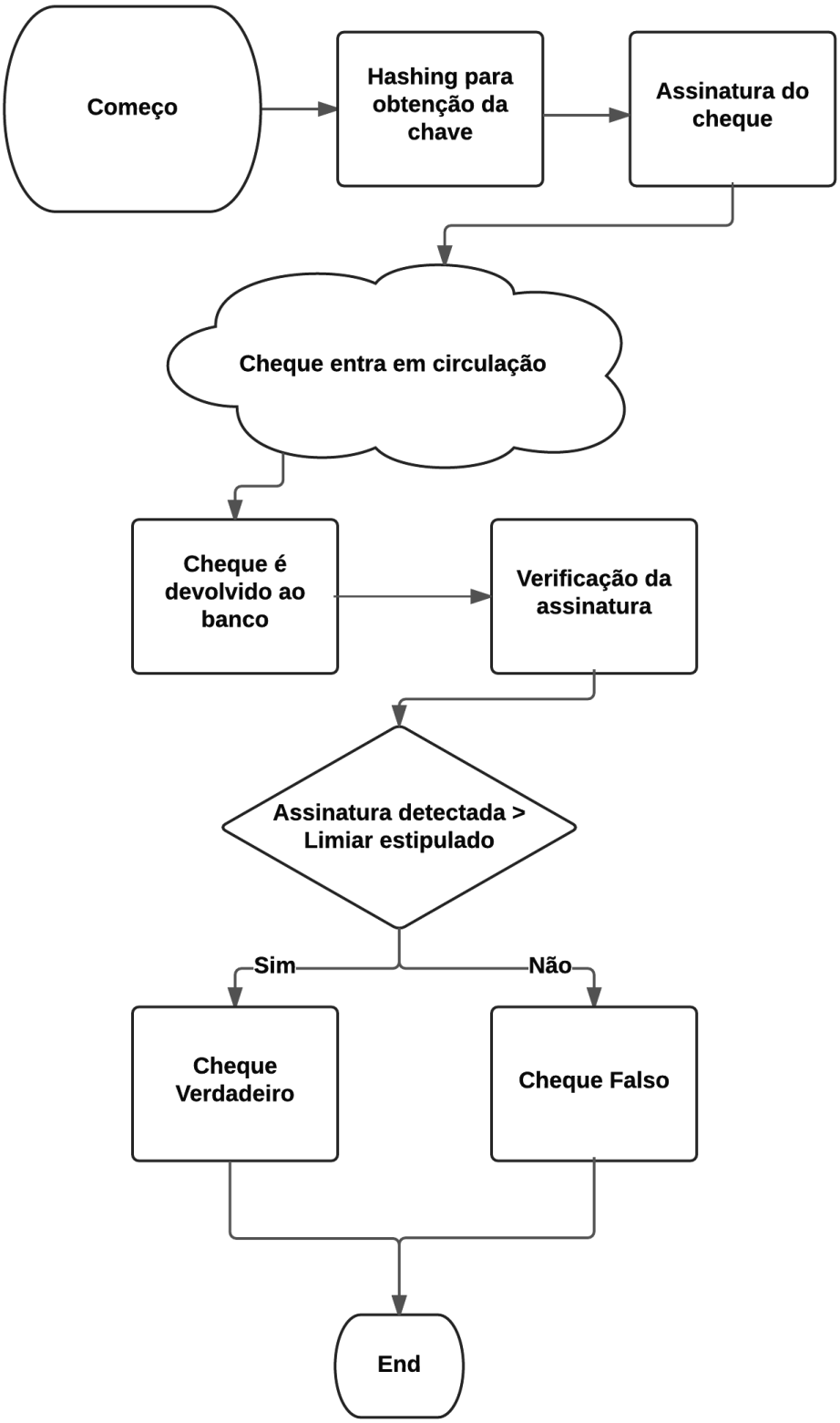


Figura 3.1: Diagrama de fluxo contendo as principais etapas do sistema proposto.

3.2 Cheque modelo

Os testes de assinatura digital precisavam ser realizados em uma imagem controlada e com o mínimo de imperfeições o possível. Para isso, criou-se digitalmente um cheque modelo. O modelo possui características desejáveis, como grande área de fundo, com espaços para se inserir a assinatura e uma figura de fundo abstrata, de modo a dificultar a identificação da assinatura.

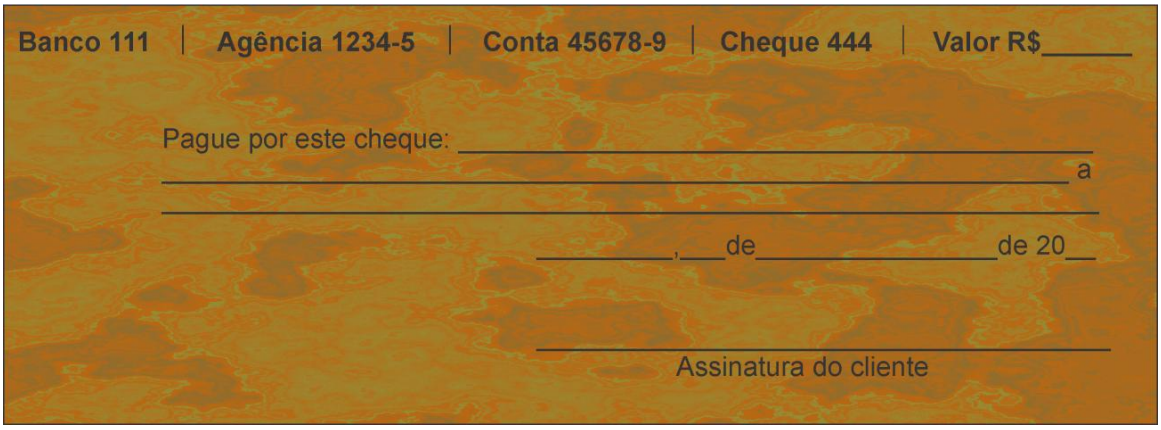


Figura 3.2: Cheque modelo.

No cheque modelo, foram realizados todos os testes de modo a desenvolver uma técnica satisfatória, que depois seria testada e adaptada para cheques reais.

O cheque modelo desenvolvido também levou em conta as características e proporções de um cheque real. Uma folha de cheque real mede 21cm de largura por 7,6cm de altura, em uma área de aproximadamente 160 cm² [4].

Ao digitalizar um cheque real em um equipamento doméstico, com resolução padrão de 300 dpi (*dots per inch*), a imagem digitalizada tinha como tamanho 4,76 MB (Mega Bytes). O cheque modelo foi desenvolvido com esse limite de tamanho, para refletir com maior precisão a realidade que se deseja simular.

3.3 Delimitação do cheque

Grande parte da área dos cheques não pode conter a assinatura digital. As partes do cheque que são preenchidas pelo usuário (cliente bancário) fogem ao controle da técnica desenvolvida, o que possivelmente induziria resultados incorretos.

Para contornar o problema do preenchimento dos cheques, além da técnica de controle de erros implementada, foi definido previamente as áreas do cheque que receberiam a assinatura digital. Como pode ser visto a seguir.

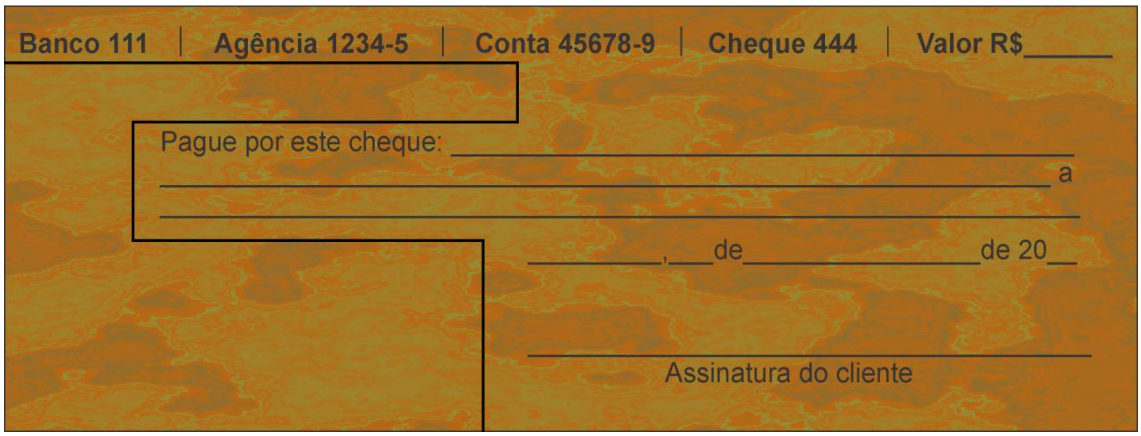


Figura 3.3: Delimitação da área assinável do cheque modelo.

A área à esquerda da delimitação mostrada na figura 3.2 é considerada a área de segurança, em que a inserção e posterior detecção da assinatura digital acontecerão sem grande interferência.

3.4 Chave

Um dos pontos centrais da técnica desenvolvida nesse trabalho é que cheques diferentes precisariam ter assinaturas diferentes. Desse modo, um possível fraudador, em posse de um cheque válido, não conseguiria produzir um segundo cheque válido apenas alterando o número sequencial do mesmo.

Para garantir uma virtual unicidade das assinaturas, foi preciso utilizar na formação da chave do *hashing* informações como: número do banco, número da agência, número da conta e número sequencial do cheque. Dessa forma, garantimos que a chave utilizada no hashing seja única.

Os números formadores da chave são combinados através de operações aritméticas, e concatenados, resultando em um número único com 20 dígitos.

Utilizando o número gerado como chave do *hashing*, conseguimos fazer com que uma mínima alteração em qualquer dos elementos formadores da chave provoque uma alteração substancial no resultado final do *hashing*.

3.5 Hashing

A função *hashing* utilizada nesse trabalho foi a *DataHash()*, implementada por Jan Simon, da Universidade de Heidelberg, e disponibilizada no ambiente *Matlab®*. Essa implementação da função *hashing* permite que o usuário defina a chave utilizada, o tipo de saída, e o tipo de função *hashing*. O tipo de função escolhida foi o MD5.

O resultado obtido é um número muito grande, que é truncado em partes menores. Cada uma dessas partes vai representar uma das informações que se deseja randomizar na metodologia de assinatura.

3.6 Assinatura

Como no trabalho de Nguyen [16], decidiu-se por assinar a imagem tendo em vista as características da visão humana. A visão humana consegue trabalhar bem com contraste e brilho, mas não é tão eficaz na distinção de cores. Para explorar essa percepção de cores não muito apurada, a assinatura será inserida em apenas uma das componentes de cores da imagem RGB.

O resultado da função hashing é utilizado para dois propósitos no processo de assinatura, determinar onde será inserida a assinatura e qual componente de cor será assinada.

Tomando como base a delimitação do cheque feita anteriormente, subdividiu-se a área assinável do cheque em nove subáreas. Cada uma dessas subáreas receberia oito alterações, em blocos (conjuntos de *pixels*) definidos pela função *hashing*. Dividindo o cheque em subáreas, garantiu-se que as 72 alterações não pudessem ser agrupadas em um único espaço da imagem, o que deixaria a assinatura mais visível. O resultado da função *hashing* é utilizado para obter as 72 coordenadas *(X, Y)* dos *pixels* centrais dos blocos de alteração dessas subáreas, em conjunto com um algoritmo para evitar colisões (duas ou mais alterações sobrepostas).

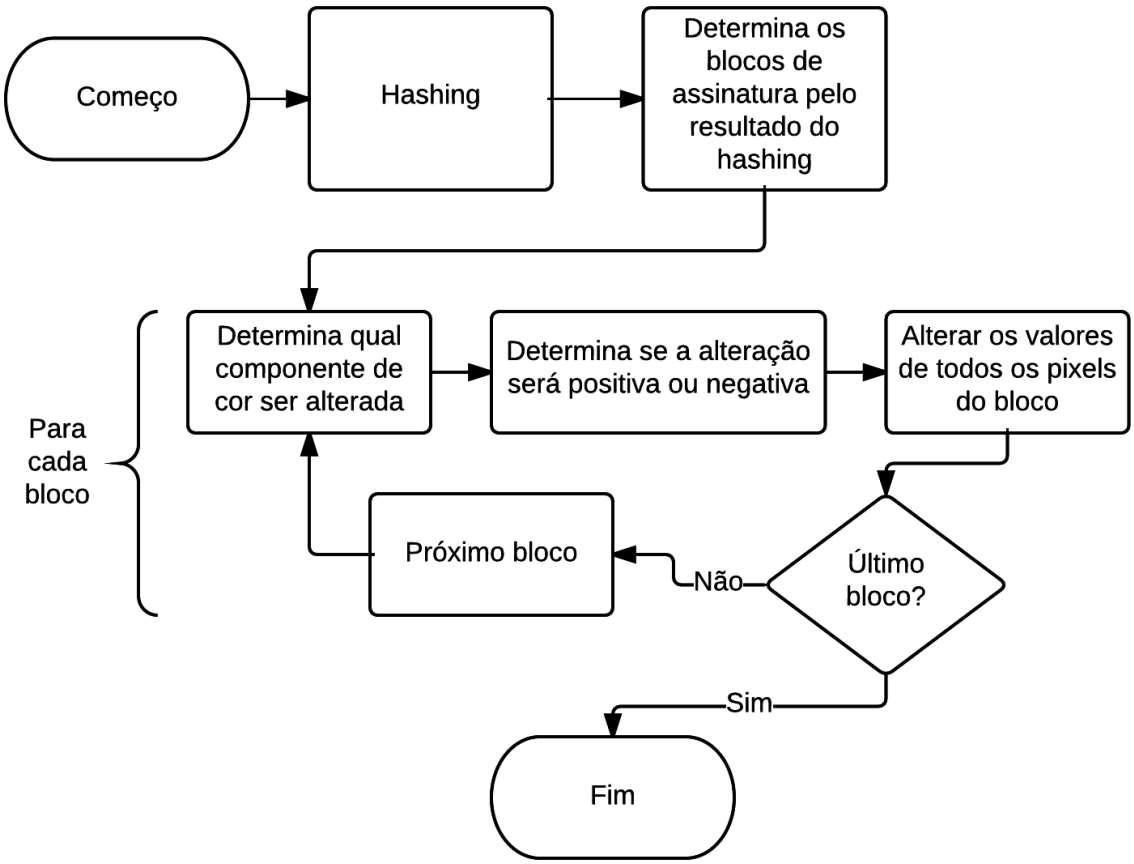


Figura 3.4: Diagrama do processo de assinatura.

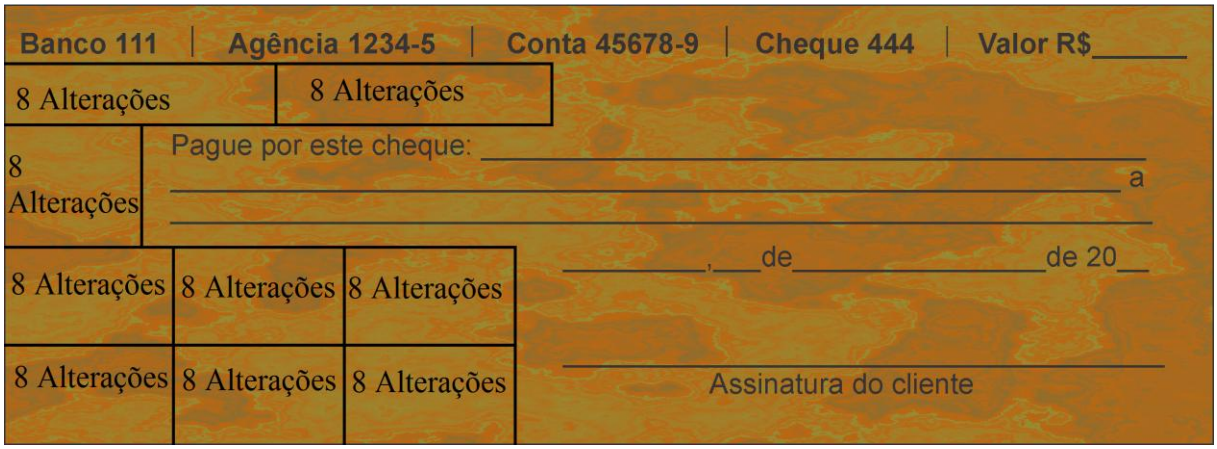


Figura 3.5: Delimitação das subáreas assináveis do cheque modelo.

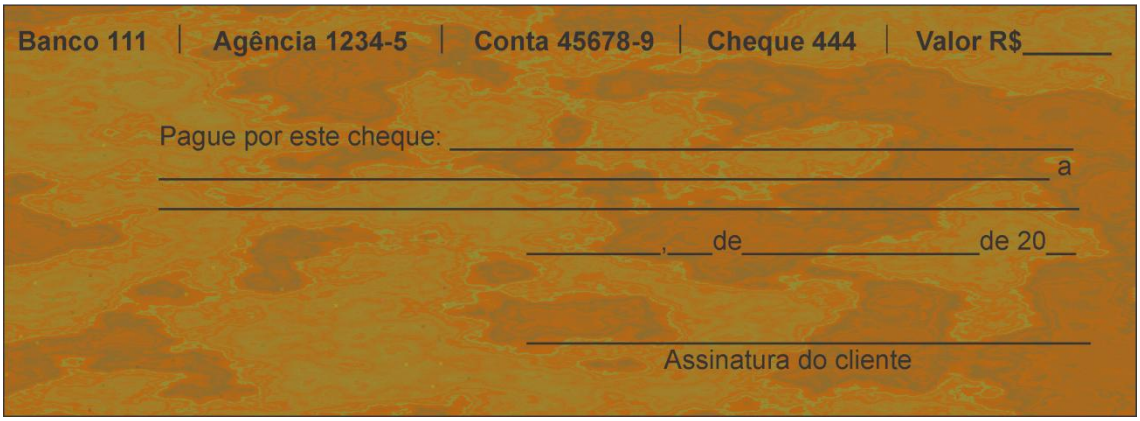
Após determinar onde será inserida a alteração, defini-se qual componente de cor será alterada. Mais uma vez o resultado da função *hashing* é utilizado para randomizar a alteração, obtendo a componente *Z* de cada bloco de *pixels* que será alterado.

Portanto, *V = (Xc, Yc, Z)*, onde *Xc* e *Yc* são as coordenadas centrais randomizadas pela função *hashing* e *Z* a componente também randomizada pela função *hashing*, *V* é o valor do *pixel* central de um bloco na componente *Z* antes da alteração (imagem original). O valor de *V* pode variar entre 0 e 255, e foi preciso inserir uma alteração nesse valor, obtendo o valor de *Va* (*V* alterado).

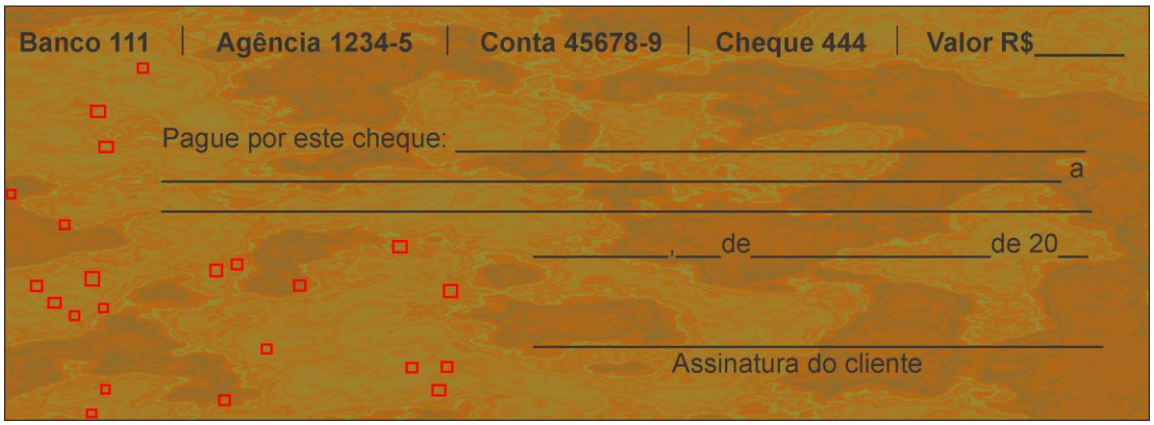
Deseja-se evitar os valores extremos, já que por hipótese eles se destacariam mais na visão humana. Assim, definimos A como o valor absoluto da alteração, com valores calculados empiricamente, e temos:

$$Va = \begin{cases} V + A, & se\ V < 127 \\ V - A, & caso\ contrário \end{cases} \tag{3.1}$$

Definiu-se *B* como o tamanho do bloco de alteração. Então *V* foi alterado para *Va* nos *pixels* centrais obtidos pela função *hashing* e nos *pixels* que compõem o bloco de alteração, de *(Xc-B, Yc-B, Z)* até *(Xc+B, Yc+B, Z)*.



(a)



(b)

Figura 3.6: Assinatura digital no cheque modelo. (a) Cheque modelo com a assinatura digital. (b) Cheque modelo com assinatura digital e marcações indicando alguns dos pontos que receberam alteração.

O processo de assinatura se repete para os demais blocos, se encerrando quando todos os 72 blocos estiverem assinados.

3.7 Inserção de Ruídos

Antes de submeter a imagem assinada aos testes de verificação, insere-se na imagem ruídos que tentam simular o ciclo de vida real do cheque.

O primeiro passo é simular a impressão do cheque, etapa fundamental, visto que é nesse momento que a imagem sai do mundo digital e entra no mundo físico. Simulou-se a impressão do cheque utilizando a *função dither* proposta por Robert W. Floyd e Louis Steinberg e implementada no ambiente *Matlab®*.

O *dither*, quando aplicado na imagem, dilui a informação de cada *pixel* em seus vizinhos, dando a impressão visual de uma imagem borrada.

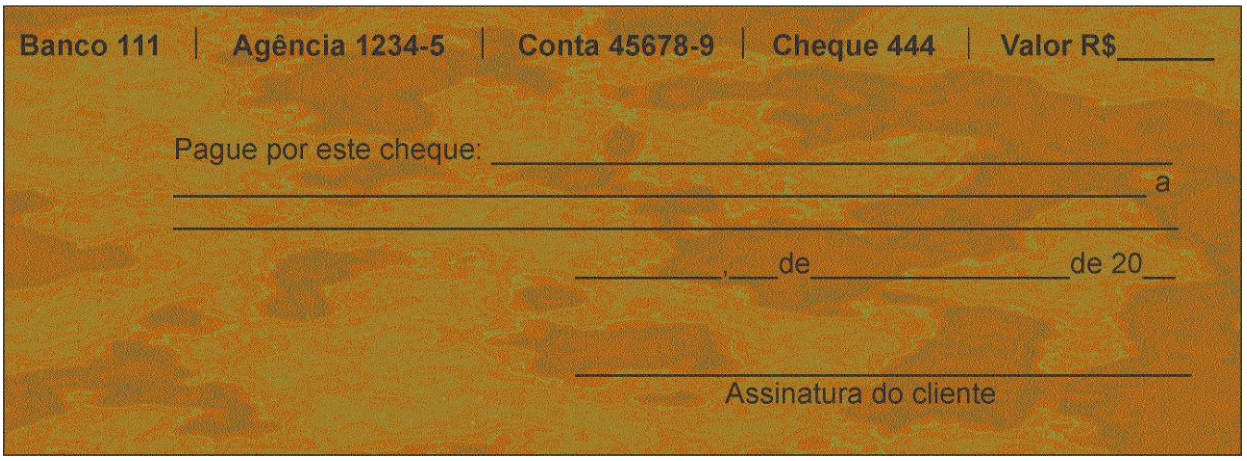


Figura 3.7: Cheque *modelo dither*.

Após a simulação da impressão, é preciso simular a digitalização do cheque, quando ele volta para o universo digital após ter sido utilizado pelo cliente bancário. Nesse ponto, rotaciona-se a imagem do cheque em *R* graus, sendo R um dos argumentos da técnica, de maneira a reproduzir um possível erro de posicionamento do cheque na máquina digitalizadora. Empiricamente percebemos que com R = 5º reproduzimos uma rotação acentuada na imagem.

Aplica-se, então, um algoritmo de *dither reverso* na imagem, que representa o processo de digitalização. Esse algoritmo calcula cada *pixel* da imagem como a média dos *pixels* ao seu redor, funcionando como um filtro de média. Ao desenvolver esse algoritmo, incluiu-se nele um parâmetro *BDR* (Bloco *Dither Reverso*), que indica quantos *pixels* vizinhos ao *pixel* central serão utilizados para calcular o valor do *pixel* central.

$$V\,(Xc,\ Yc,\ Z) = \frac{\sum_{x=-BDR}^{BDR}\sum_{y=-BDR}^{BDR} V(Xc+x, Yc+y, Z)}{(2BDR+1)^2} \qquad (3.2)$$

O valor ideal de *BDR* depende da propagação de erro causada pelo processo de *dither*. Quanto maior tiver sido a propagação, em mais *pixels* vizinhos ao pixel central vai estar diluída a informação original, e maior deverá ser o *BDR*. Experimentalmente se obteve o valor ideal de *BDR = 3* para a função de *dither* utilizada.

Por fim, rotaciona-se a imagem em *–R graus*, revertendo o erro de posicionamento anteriormente inserido.

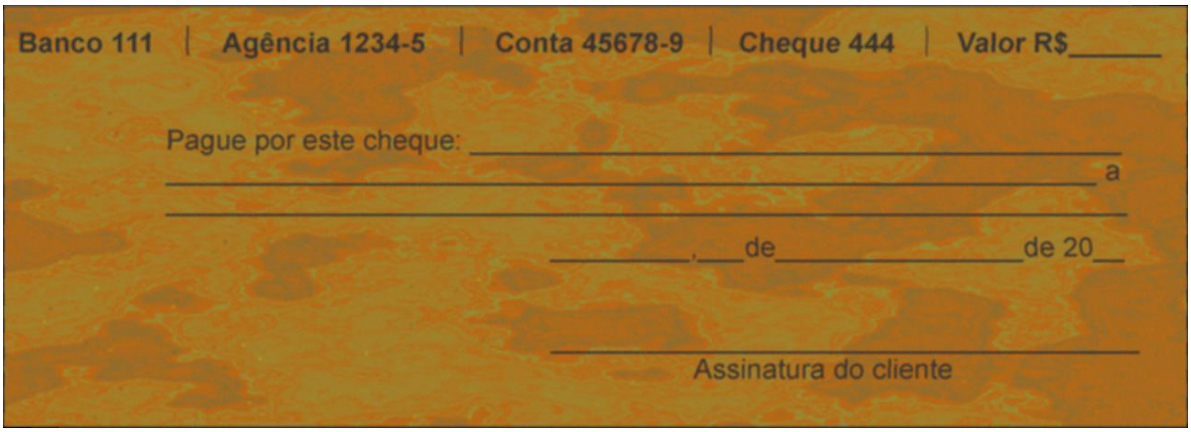


Figura 3.8: Cheque modelo após a retirada dos ruídos.

Ao fim desse processo foi obtida a imagem digitalizada do cheque assinado, que deve seguir para o processo de verificação da assinatura, de modo a ser validado como verdadeiro ou recusado como falso.

3.8 Conferência da Assinatura

O processo de conferência da assinatura é análogo ao de assinar a imagem. De posse dos dados bancários básicos que compõem a chave, a função *hashing* é recalculada.

Os *pixels* centrais dos blocos de assinatura são recuperados, bem como a componente de cor Z em que se espera verificar a assinatura em cada um desses blocos. Os valores dos blocos no cheque que está sendo conferido (cheque motivo) são comparados com os valores dos blocos correspondentes no cheque padrão, sem assinatura alguma (cheque modelo).

Avalia-se primeiramente em cada bloco, se a alteração examinada é positiva ou negativa, ou seja, se o valor do *pixel* central do bloco $V = (Xc, Yc, Z)$, no cheque modelo é < 127, *ou* $>= 128$ respectivamente.

No processo de assinatura, assinou-se o *pixel* central, e os *B pixels* a sua volta, sendo a assinatura formada por blocos. Como o processo de *dither* causa a propagação de erros, a alteração inserida nos *pixels* mais afastados do centro do bloco são mais afetadas por essa interferência.

No processo de verificação de assinatura, foi utilizado o parâmetro *BV* (Bloco de Verificação), que representa o tamanho do bloco em que a assinatura deve ser verificada. *BV*

deve ser < = *B*, de modo que, se *BV* = *B*, verifica-se a assinatura exatamente onde ela foi inserida, e se *BV* < *B*, estamos verificando a assinatura apenas nos *pixels* mais centrais do bloco de assinatura original.

Calcula-se a média dos valores dos *pixels* dos blocos de verificação, obtendo a *MBD* (Média do Bloco Modelo) e a *MBT* (Média do Bloco Motivo) para cada bloco de assinatura.

Define-se, então, *Ad* (Alteração detectada):

$$Ad = \begin{cases} MBT - MBD, \ se\ alteração\ positiva \\ MBD - MBT, \ caso\ contrário \end{cases} \tag{3.3}$$

Na Imagem modelo temos:

$$\text{MDB} = \frac{\sum_{x=-bv}^{bv}\sum_{y=-bv}^{bv} V(Xc+x,Yc+y,Z)}{(2bv+1)^2} \tag{3.4}$$

Na imagem motivo:

$$\text{MBT} = \frac{\sum_{x=-bv}^{bv}\sum_{y=-bv}^{bv} V(Xc+x,Yc+y,Z)}{(2bv+1)^2} \tag{3.5}$$

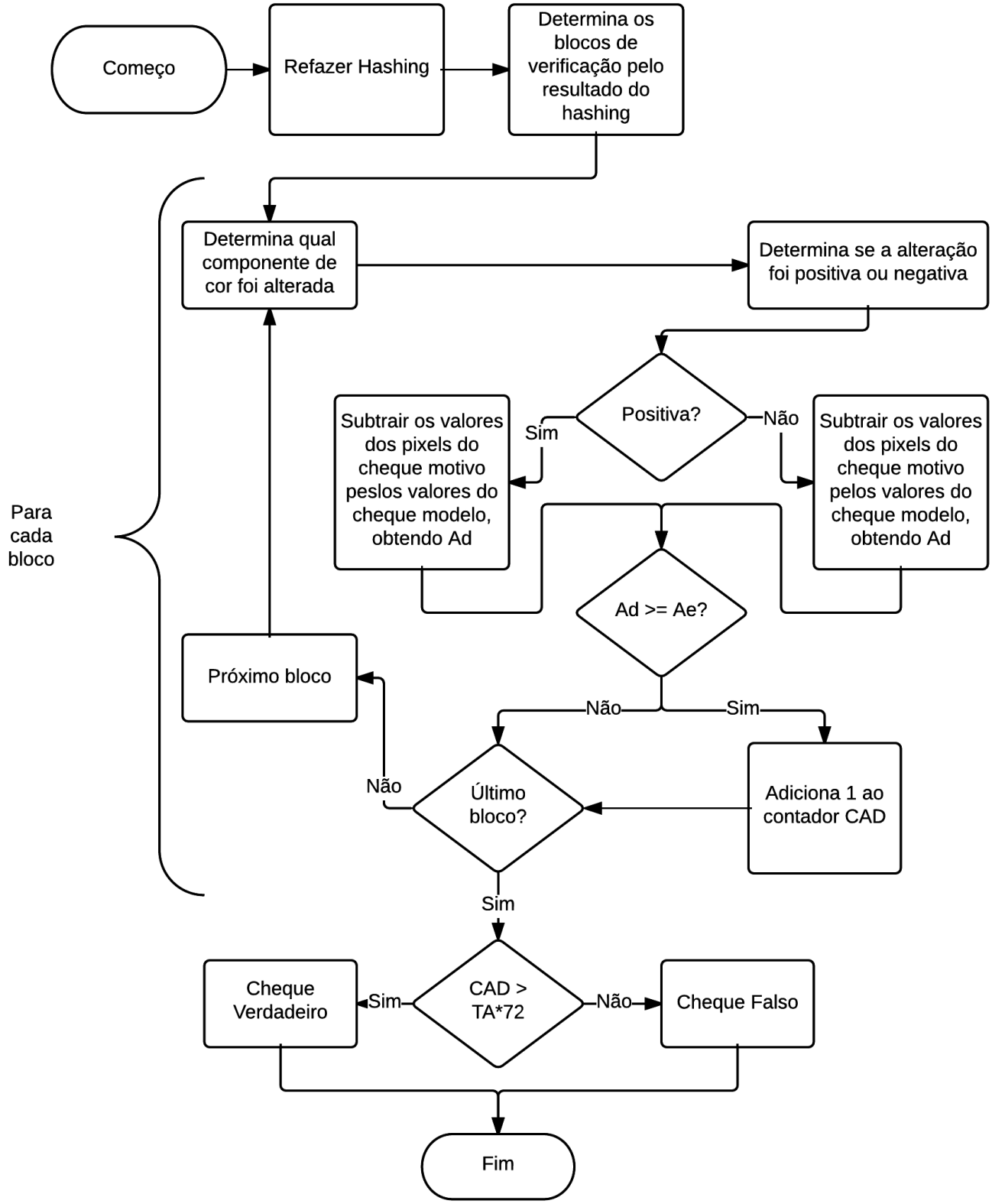


Figura 3.9: Diagrama do processo de conferência da assinatura.

Cada *Ad* calculada é comparada com a *Ae* (Alteração esperada em %) definida empiricamente e passada como parâmetro. O ruído, presente em todo o processo de assinatura e conferência de assinatura, modifica a alteração inserida na imagem. O valor definido para *Ae* deve levar em conta essa modificação, de modo que valores levemente inferiores à alteração *A* inicialmente inserida sejam aceitos como válidos.

Percorremos então todos os blocos, computando as alterações em CAD (Contador Alterações Detectadas):

$$\begin{cases} CAD = CAD + 1, se\ Ad \geq Ae * A \\ \text{pula para o próximo bloco, caso contrário} \end{cases} \tag{3.6}$$

Para cada *Ad >= Ae * A*, tem-se uma alteração valida, e esta é computada em CAD.

Ao final do processo de verificação de assinatura, *CAD* vai ter um valor variando de 0 a 72, sendo que no primeiro extremo nenhuma alteração será validada e no segundo extremo todas as alterações serão validadas. Por fim, compara-se o *CAD* com uma *TA* (Taxa de Aceitação em %) passada como parâmetro, para validar ou não o cheque. Se *CAD >= TA * 72*, cheque válido; caso contrário, cheque falso.

Os valores de *TA* e *Ae*, devem ser cuidadosamente escolhidos, pois valores muito brandos desses dois parâmetros podem levar a falsos positivos (cheques falsos sendo aceitos) e valores muito rígidos podem levar a falsos negativos (cheques verdadeiros sendo rejeitados).

3.9 Verificação de Fraude

Analisando a metodologia de assinatura e conferência de assinatura proposta, verificou-se uma vulnerabilidade. Um fraudador, sem conhecer a chave *hashing*, mas sabendo como as alterações são inseridas no cheque, poderia assinar o cheque por inteiro. Ao assinar o cheque por inteiro, o fraudador teria uma chance significativa de conseguir ter o cheque validado.

Para evitar esse tipo de ataque, implantou-se um processo de verificação de não assinatura. Esse processo utiliza uma área de segurança que não pode receber assinaturas, e verifica a presença de alteração em pontos específicos dessas áreas.

Para verificar a presença de alteração nesses pontos, é utilizada a mesma metodologia da verificação de assinatura, em que o valor obtido nos *pixels* do cheque motivo é comparado com o valor obtido no cheque modelo.

A procura por alterações nos pontos em que não se devem ter assinaturas é feita nas três componentes de cor separadamente. Se qualquer dos pontos verificados tiver *Ad* >= *Ae*, em qualquer das componentes de cor, o cheque é considerado falso.

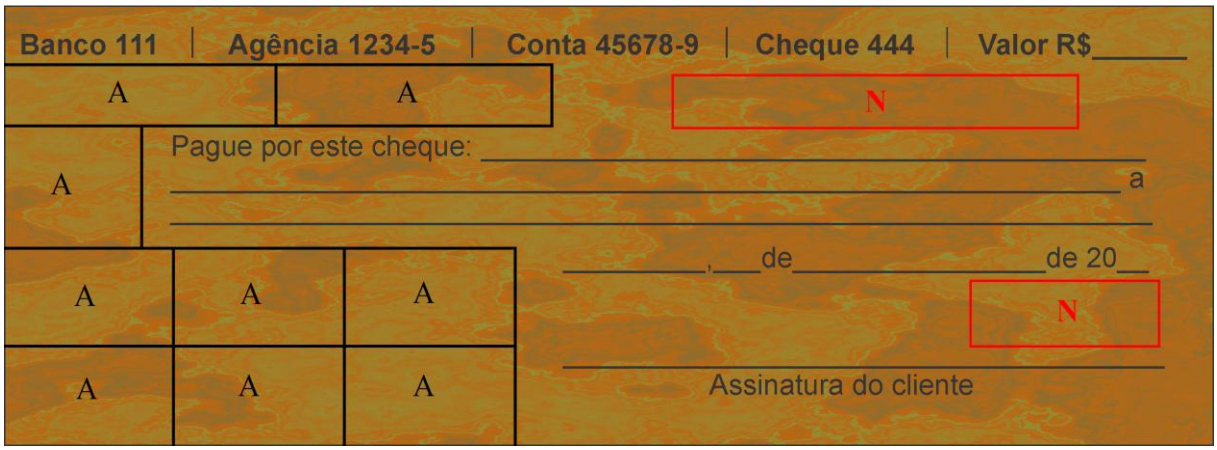


Figura 3.10: Cheque modelo com indicações das áreas assináveis e não assináveis. As áreas indicadas em preto com a letra A, são as áreas assináveis nas quais ocorrem o processo de assinatura e verificação de assinatura. As áreas indicadas em vermelho com a letra N são as áreas não assináveis em que ocorre a verificação de fraude

Capítulo 4

Resultados Experimentais

Neste capítulo serão apresentados os resultados obtidos quando se aplicou a metodologia de assinatura e conferência de assinatura no cheque modelo desenvolvido. Após a apresentação dos resultados no cheque modelo, serão dados os resultados obtidos em um cheque real digitalizado.

4.1 Testes com cheque modelo

Para testar a metodologia desenvolvida, foi gerada uma base de testes com 60 cheques modelo. Esses 60 cheques divergiam entre si nas informações utilizadas pela metodologia para definir a chave do *Hashing*. Portanto, essa base de testes possui cheques de clientes diversos, contas diversas, agências diversas e bancos diversos.

Com a base de testes gerada, cada um dos 60 cheques foi assinado, conforme a metodologia proposta. Além disso, cada um deles foi, então, submetido ao processo de verificação de assinatura com os dados dele mesmo e dos outros 59 cheques.

Quando o cheque é submetido à verificação com os dados dele mesmo, está sendo testado o uso correto do cheque, e espera-se que o cheque seja validado pelo sistema. Na situação em que o cheque é submetido à verificação com os dados dos outros cheques está sendo testada uma fraude, e espera-se que o cheque seja invalidado pelo sistema.

Esse processo de assinar 60 cheques e verificar cada um deles 60 vezes resulta em 3600 testes sendo realizados (60x60). Esses 3600 testes formam uma bateria de testes. A reposta ideal para uma bateria de teste é de 60 testes válidos (quando os cheques foram

testados com seus dados verdadeiros), e os 3540 testes restantes (quando os cheques foram testados com os dados dos outros cheques) inválidos.

Foram realizadas 6 baterias de testes, alterando os parâmetros utilizados entre elas, de modo a verificar o comportamento do método proposto com parâmetros mais e menos rígidos. Abaixo estão listados os parâmetros dos testes realizados, juntamente com uma imagem de um cheque assinado com esses parâmetros.

4.1.1. Bateria de Testes 1

Parâmetros utilizados:

A = 25; Ae = 15; B = 3; Bdr = 3; Bv = 1; R = 0; TA = 51.

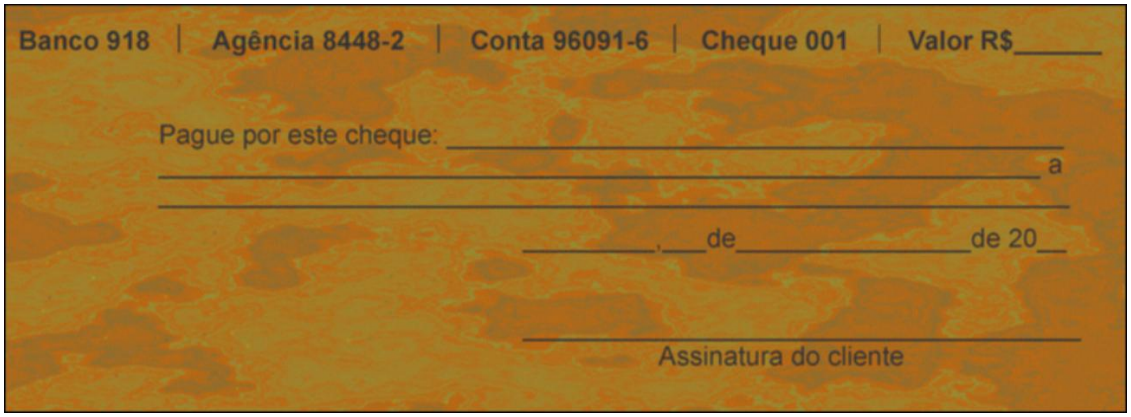


Figura 4.1: Cheque assinado com parâmetros do Teste 1

4.1.2. Bateria de Testes 2

Parâmetros utilizados:

A = 25; Ae = 15; B = 2; Bdr = 2; Bv = 2; R = 0; TA = 51.

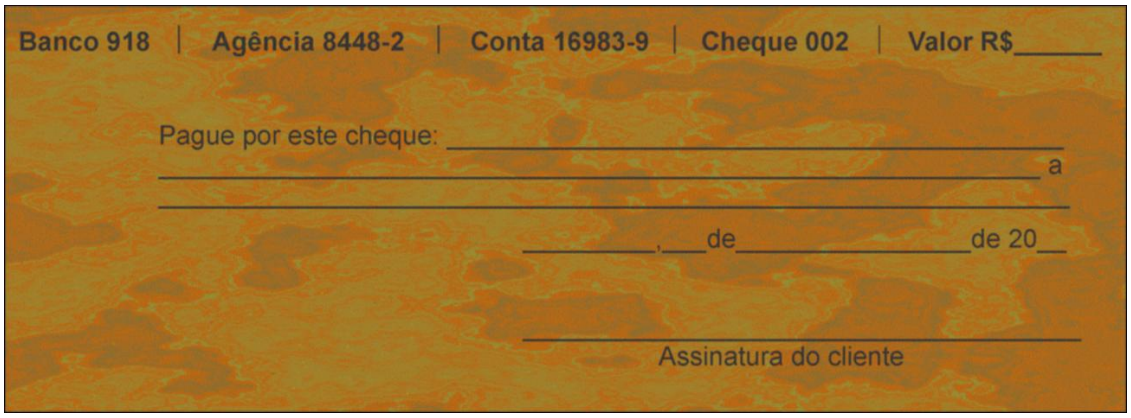


Figura 4.2: Cheque assinado com parâmetros do Teste 2

4.1.3. Bateria de Testes 3

Parâmetros utilizados:

A = 15; Ae = 09; B = 2; Bdr = 2; Bv = 2; R = 0; TA = 58.

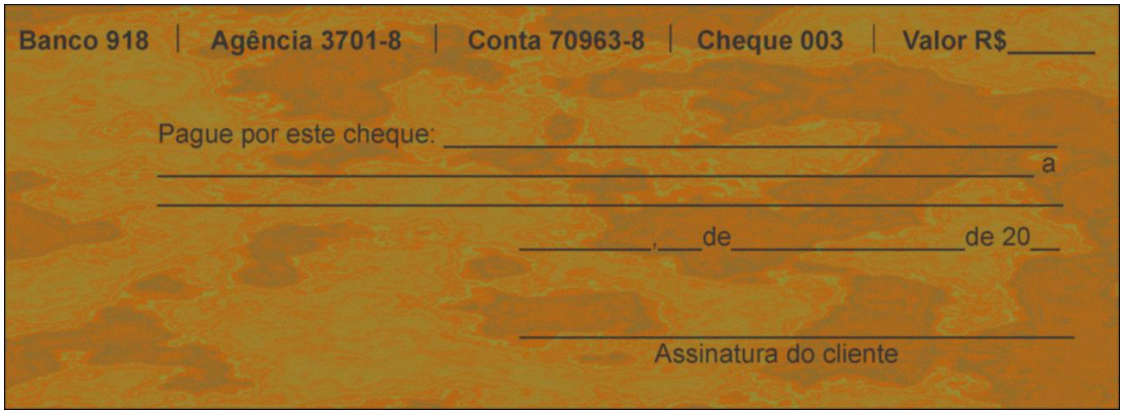


Figura 4.3: Cheque assinado com parâmetros do Teste 3

4.1.4. Bateria de Testes 4

Parâmetros utilizados:

A = 25; Ae = 15; B = 2; Bdr = 1; Bv = 1; R = 0; TA = 51.

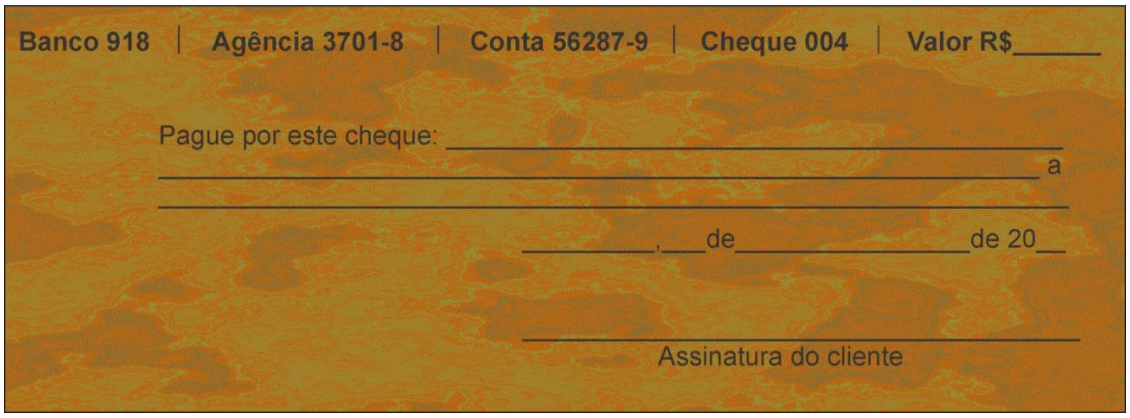


Figura 4.4: Cheque assinado com parâmetros do Teste 4

4.1.5. Bateria de Testes 5:

Parâmetros utilizados:

A = 30; Ae = 18; B = 3; Bdr = 3; Bv = 1; R = 1; TA = 51.

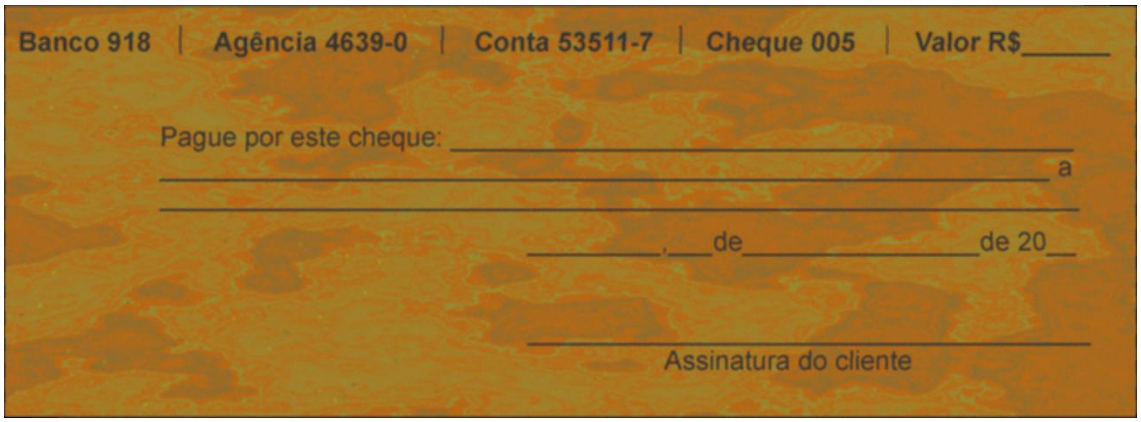


Figura 4.5: Cheque assinado com parâmetros do Teste 5

4.1.6. Bateria de Testes 6

Parâmetros utilizados:

A = 30; Ae = 18; B = 3; Bdr = 3; Bv = 1; R = 5; TA = 51.

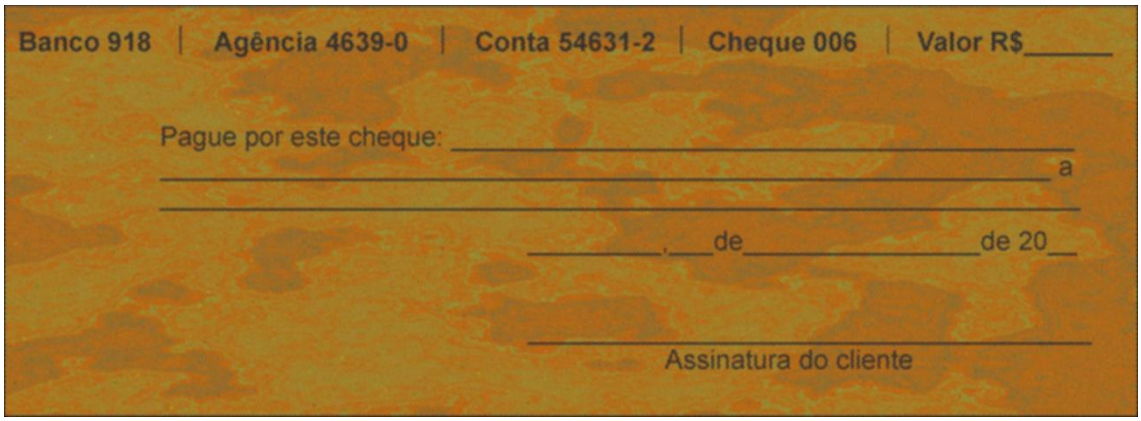


Figura 4.6: Cheque assinado com parâmetros do Teste 6

Para testar o processo de verificação de fraude descrito anteriormente, assinou-se um cheque por completo, e o submeteu ao mesmo processo de verificação de assinatura. O sistema foi capaz de identificá-lo como falso, através do processo de verificação de fraude, que busca alterações em áreas indevidas.

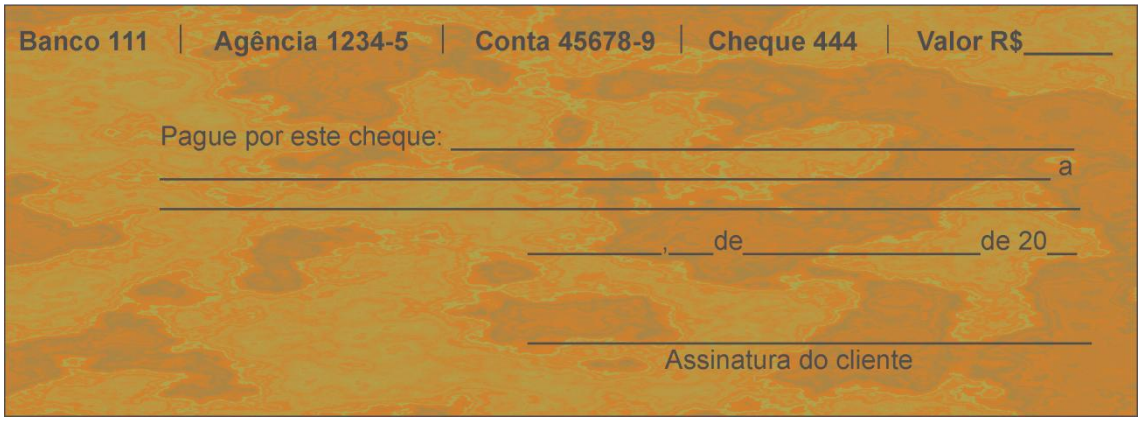


Figura 4.7: Cheque falso assinado por completo

4.1.7. Tabela 01: Resumo dos resultados com cheque modelo

Parâmetro	Valor mínimo	Valor máximo
Alteração (A)	25	30
Alteração esperada (Ae)	70%	70%
Bloco da Assinatura (B)	2	3
Bloco do Dither Reverso (Bdr)	1	3
Bloco de Verificação (Bv)	1	2
Rotação (R)	0	5
Taxa de aceitação (Ta)	70%	80%
Baterias de testes realizadas	6	
Baterias com falsos positivos	0	
Baterias com falsos negativos	2	

Tabela 4.1: Resultados dos testes com cheque modelo

4.2 Análise dos resultados com cheque modelo

Observa-se, pelos resultados obtidos, que o sucesso da metodologia depende muito dos valores escolhidos para os parâmetros. Observou-se falsos negativos quando a rigidez dos parâmetros é forçada, mas não foi obtido falsos positivos nos testes.

Ao diminuir o parâmetro A, o sistema passa a não conseguir identificar a assinatura com a precisão desejada. Por outro lado, um aumento significativo do valor de A tem como efeito colateral uma visibilidade maior da assinatura ao olho humano. Para contornar esses problemas é preciso combinar o incremento de A coma redução dos parâmetros relacionados à tamanho de bloco (B, Bdr e Bv), ou combinar a redução de A com a redução dos parâmetros relacionados as taxas de aceitação da assinatura (Ta e Ae).

O parâmetro B também está relacionado com a visibilidade das alterações feitas na imagem. Faz-se necessário balancear o aumento de B e o aumento de A, para não tornar a assinatura muito visível.

A Ta está diretamente ligada ao sucesso da verificação. Um leve aumento em Ta, gerou como consequência falsos negativos, na bateria de testes 3.

No processo de *dither* reverso, o parâmetro Bdr tem papel importante na preservação da assinatura, além da manutenção da nitidez da imagem. É possível observar que as imagens 4.3 e 4.4 são menos nítidas do que as demais, provavelmente por conta da alteração em BDR.

Conforme esperado, observou-se que o Bv deve ter um valor baixo, de maneira a ignorar os erros maiores que serão inseridos nos pixels limites da assinatura.

Também foi notado que a rotação R, inserida na imagem como ruído, pouco interferiu na verificação da assinatura. Era esperado obter resultados ruins ao inserir a rotação na imagem, mas a metodologia se mostrou capaz de suportar esse tipo de ruído.

Além dos testes de verificação da assinatura pelo sistema, foram realizados testes básicos de detecção visual da assinatura com cerca de 10 pessoas. Nesses testes as imagens de um cheque assinado e um cheque sem assinatura eram colocados lado a lado e a pessoa deveria dizer de havia diferenças entre as imagens e tentar identificar quais eram essas diferenças. As pessoas testadas não foram capazes de perceber diferenças entre as imagens.

As imagens 4.1 a 4.6 mostram 6 cheques assinados de maneiras diferentes, utilizados nos testes de detecção visual da assinatura.

Por outro lado, o cheque completamente assinado (simulando uma fraude), da Figura 4.7, é visivelmente mais claro do que os demais cheques. Ao realizar o teste de verificação visual comparando a imagem do cheque completamente assinado com a imagem de um cheque assinado corretamente, as pessoas foram capazes de apontar a diferença entre as duas imagens.

4.3 Testes com cheque real

Após os resultados satisfatórios com o cheque modelo, foi necessário testar a metodologia proposta em um cheque real. Um cheque do Banco do Brasil foi digitalizado com resolução de 300 dpi, gerando uma imagem digitalizada de tamanho 4,76 MB.

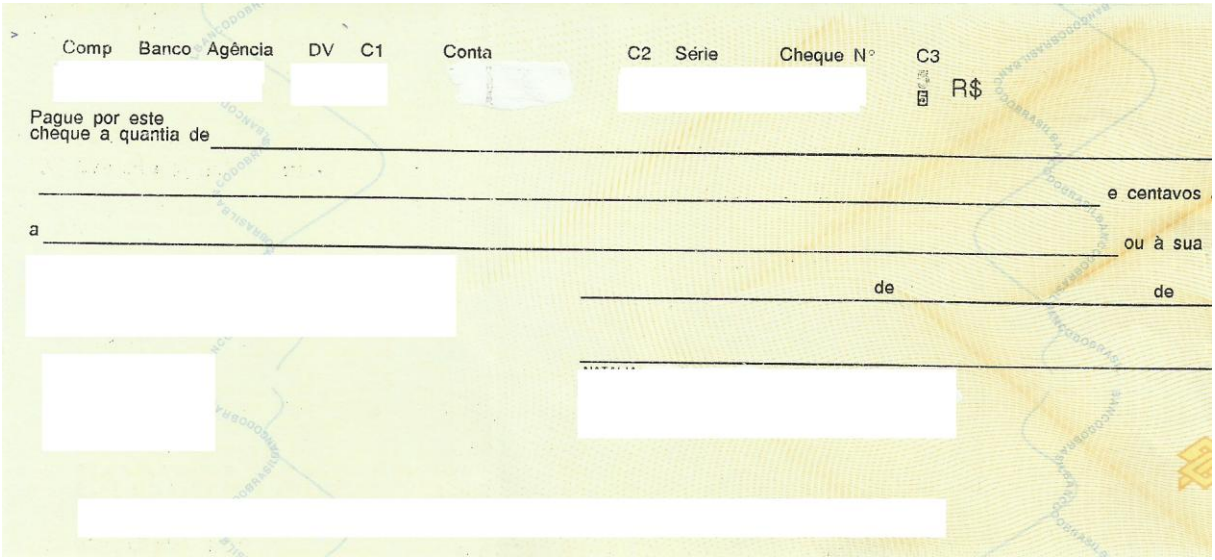


Figura 4.8: Cheque real, do Banco do Brasil, digitalizado

Depois da digitalização da imagem, foi necessário redefinir as áreas assináveis do cheque, bem como delimitar as áreas de segurança utilizadas no processo de detecção de fraudes. Observou-se, assim, que o cheque real possui mais informações e menos áreas livres de textos, o que eleva a dificuldade de camuflar a assinatura.

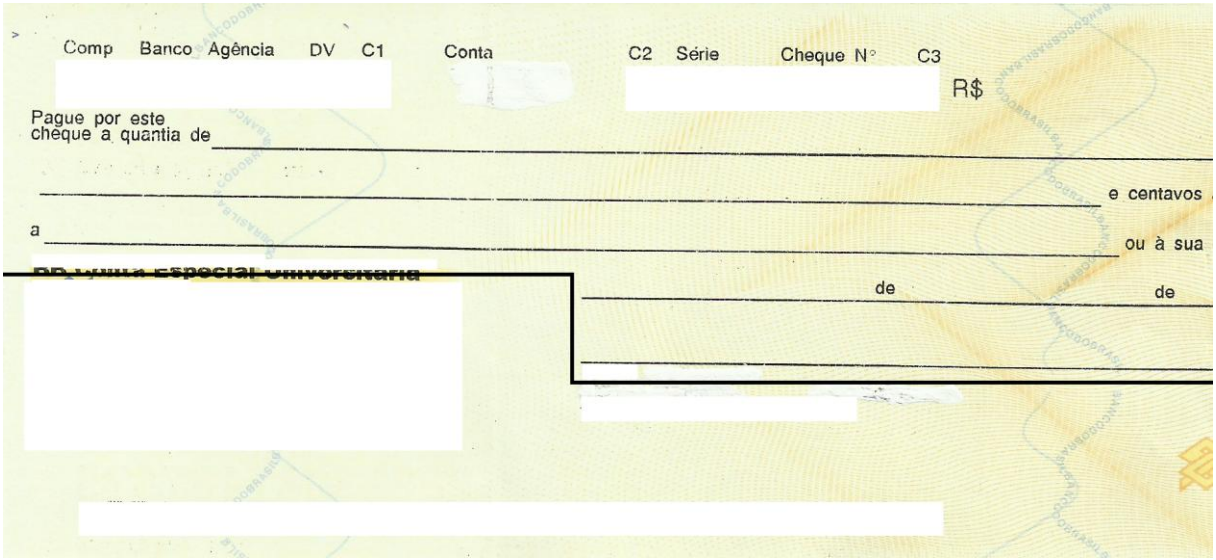


Figura 4.9: Cheque real, do Banco do Brasil, com áreas delimitadas

Com a delimitação das áreas assináveis do cheque, o mesmo foi submetido ao processo de assinatura, com o propósito de verificar se as alterações inseridas ainda continuavam imperceptíveis ao olho humano.

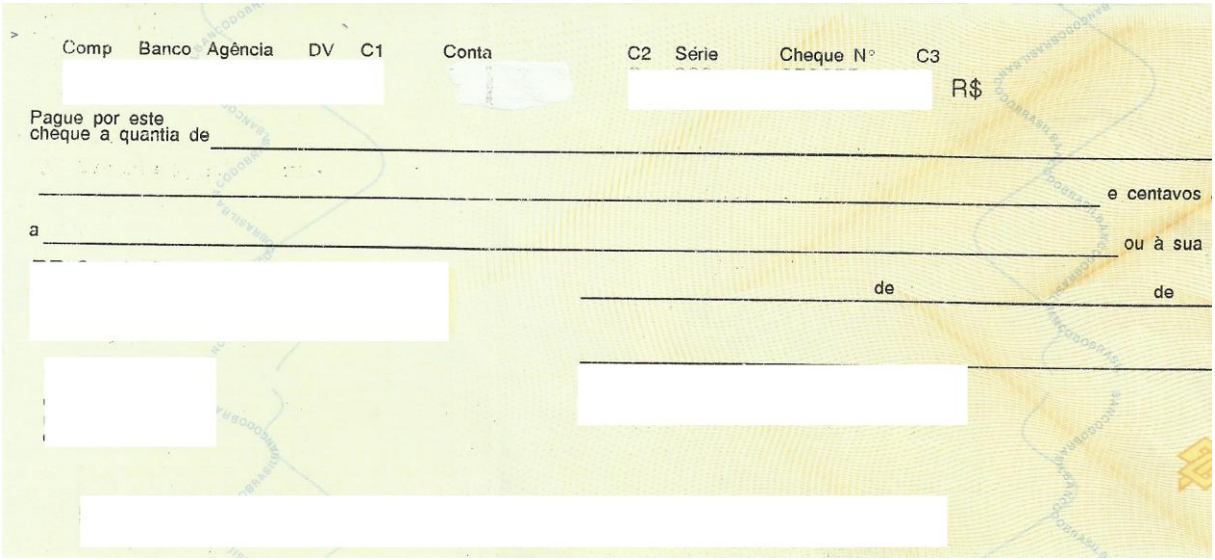


Figura 4.10: Cheque real, do Banco do Brasil, assinado

A imagem resultante do processo de assinatura ainda consegue camuflar satisfatoriamente as alterações inseridas. Então o cheque foi submetido a uma bateria de testes, os parâmetros foram variados utilizando como base as análises dos resultados com o teste modelo. Fixou-se os parâmetros $Bdr = 3$ e $Bv = 1$, pois com os testes anteriores foi possível notar um melhor desempenho quando eles estavam nesses valores, e $R = 5$, porque representa um valor elevado de erro no posicionamento da imagem e o sistema já se mostrou capaz de absorver esse valor de rotação.

4.3.1. Tabela 4.2: Resumo dos resultados com cheque real

Parâmetro	Valor mínimo	Valor máximo
Alteração (A)	8	12
Alteração esperada (Ae)	20%	50%
Bloco da Assinatura	2	3
Taxa de aceitação (Ta)	30%	50%
Baterias de testes realizadas	120	
Baterias com falsos positivos	73	
Baterias com falsos negativos	2	

Tabela 4.2: Resultados dos testes com cheque real

4.4 Análise dos resultados com cheque real

Observa-se na tabela de resultados que a metodologia proposta se comporta adequadamente a partir de uma cuidadosa escolha dos valores de parâmetros. As diferenças entre o cheque real e o cheque modelo não foram suficientes para interferir no sucesso dos testes.

Nesse segundo teste, ao variar de forma mais intensa os parâmetros, foi possível testar os limites aceitáveis para cada um deles, forçando resultados falsos negativos e falsos positivos. Com os resultados desses testes é possível definir combinações de valores seguros para os parâmetros, com os quais o método proposto não apresenta falhas.

Além disso, observa-se na tabela de resultados que os valores de *A* na bateria de testes do cheque real foram reduzidos em aproximadamente 50% em relação aos valores utilizados nos testes com cheques modelos. Isso se deve ao aumento da preocupação com a visibilidade da assinatura. A diminuição do valor desse parâmetro não prejudicou o funcionamento correto do processo, pois foi balanceado com a redução dos valores de *Ae* e *Ta*. Nota-se, também, que aumentando *B* de 2 para 3, obteve-se um número maior de casos de teste sem falsos positivos.

Por fim, mantendo *Ae = {40%, 50%}, Ta = {40%, 50%}, B = 3* e *A > = 10* temos um total de 12 baterias de teste com execução 100% correta (sem falsos positivos ou falsos negativos).

Ainda se faz necessário realizar testes com cheques de outros bancos, bem como realizar testes com cheques que foram de fato preenchidos e utilizados no mercado, para ser garantida a robustez da aplicação.

Capítulo 5

Conclusões

Inserir uma assinatura digital imperceptível ao olho humano num cheque mostrou-se um grande desafio. Essa assinatura deve resistir aos ruídos inseridos no processo de impressão e digitalização do cheque, e tais podem ser permeados por perdas irreversíveis na imagem.

Para que a técnica proposta neste trabalho atinja os objetivos, é necessário que seja feita uma cuidadosa escolha dos parâmetros utilizados. Portanto, após encontrar empiricamente os parâmetros ideais para os cheques utilizados nos testes, foi-se capaz de registrar baterias de testes com 100% de acerto.

Trabalhos futuros devem ser feitos para aprimorar a técnica e submetê-la a testes mais complexos**.** Espera-se que seja possível inserir no cheque mais metadados por meio de assinatura digital. No entanto, é necessário ainda verificar se a assinatura digital sobrevive ao manuseio do cheque pelos clientes bancários, que muitas vezes inserem rasuras em locais inesperados.

Projetos que visam à segurança na transferência de recursos financeiros devem continuar sendo realizados, de modo a tentar neutralizar as ações de atacantes que pretendem burlar o sistema. O desenvolvimento de novas técnicas de segurança é de interesse direto da sociedade.

Referências

[1] G1. Uso de cheques despenca em uma década, mas continua representativo. Gazeta do Povo, Santa Catarina, 16 out. 2010. Disponível em: <http://www.gazetadopovo.com.br/economia/uso-de-cheques-despenca-em-uma-decada-mas-continua-representativo-f27pwyga676owf7fn2mmldqa6>. Acesso em: 01 nov. 2015.

[2] Brasil. Banco Central do Brasil. FAQ – Compensação de Cheques. Brasília, mai. 2014. Disponível em: < http://www.bcb.gov.br/?COMPENSACAOCHEQUESFAQ>. Acesso em: 01 nov.2015.

[3] Dias, D. Modelo Para Representação Eletrônica de Cheques. Dissertação de mestrado, UnB, Brasília, 2006.

[4] Brasil. Banco Central do Brasil. Resolução nº 3279. Dispõe sobre a indicação da data de relacionamento de clientes de instituições financeiras em formulários de cheque. Brasília, 28 abr. 2005. Disponível em: < http://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/48432/Res_3279_v1_O.pdf >. Acesso em: 01 nov.2015.

[5] Brasil. Caixa Econômica Federal. A segurança nos cheques da Caixa. Brasília, Nov. 2015a. Disponível em: < http://www.caixa.gov.br/seguranca/cheques/Paginas/default.aspx>. Acesso em: 01 nov.2015.

[6] Gonzales, R.C.; Woods, R.E. Processamento de imagens digitais. São Paulo: Edgard Blücher, 2000. 509 p.

[7] Shannon, C. E. A Mathematical Theory of Communication. The Bell System Technical Journal, Vol. 27, pp. 379–423, 623–656, October, 1948.

[8] Sanches, I. J. Compressão sem Perdas de Projeções de Tomografia Computadorizada usando a Transformada Wavelet. Dissertação de mestrado, UFPR, Curitiba, 2001.

[9] Brasil. Instituto Nacional de Tecnologia da Informação. Quem Somos. Brasília, nov. 2015. Disponível em: <www.iti.gov.br/institucional/quem-somos>. Acesso em: 25 nov.2015.

[10] Diffie, W.; Hellman, M. E. New Directions in Crypthography. IEEE Transactions on information theory, VOL. IT-22, NO. 6, November, 1976.

[11] Oliveira, R. S. Sobre o Emprego de Tabelas Hash em Sistemas Operacionais de Tempo Real. In: 5o Workshop de Sistemas Operacionais Belém (WSO'2008). 5. Belém – PA, 15 e 16 de Julho de 2008.

[12] Rivest, R. The MD5 Message-Digest Algorithm. Internet Report, RFC 1321, Apr. 1992.

[13] Spencer, W. T. Efficient Inverse Color Map Computation. In: Graphics Gems II, Academic Press, 1991, pag. 75.

[14] Wolfgang, R. B.; Delp, E. J. A Watermarking Technique for Digital Imagery: Further Studies. Center for Education and Research in Information Assurance and Security, Purdue University, West Lafayette, IN 47907-2086, CERIAS Tech Report 2001.

[15] Brassil, J. T.; Low, S. Maxemchuck, N. F.; O'Gorman, L. Eletronic Marking and Indentification Techniques to Discourage Document Copying. IEEE Journal on sel, Areas in communication, NO. 8, 1495-1504, 1995.

[16] Canh, H. V.; Nguyen, L. V.; Tien T. N. A Watermarking Method Robust For Copyright Protection of Images Against Print-Scan. International Conference on Information Science and Control Engineering (ICISCE 2012), IET, IN 14031130, Shenzhen, 7-9 Dec. 2012.

Apêndice

Apêndice I: Tabelas dos testes com cheque modelo

Tabela I.1: Teste 1	
Parâmetro	Valor
Alteração (A)	25
Alteração esperada (Ae)	70%
Bloco da Assinatura (B)	3
Bloco do Dither Reverso (Bdr)	3
Bloco de Verificação (Bv)	2
Rotação (R)	0º
Taxa de aceitação (Ta)	70%
Falsos Positivos	0
Falsos Negativos	0

Tabela I.2: Teste 2	
Parâmetro	Valor
Alteração (A)	25
Alteração esperada (Ae)	70%
Bloco da Assinatura (B)	2
Bloco do Dither Reverso (Bdr)	2
Bloco de Verificação (Bv)	2
Rotação (R)	0º
Taxa de aceitação (Ta)	70%
Falsos Positivos	0
Falsos Negativos	0

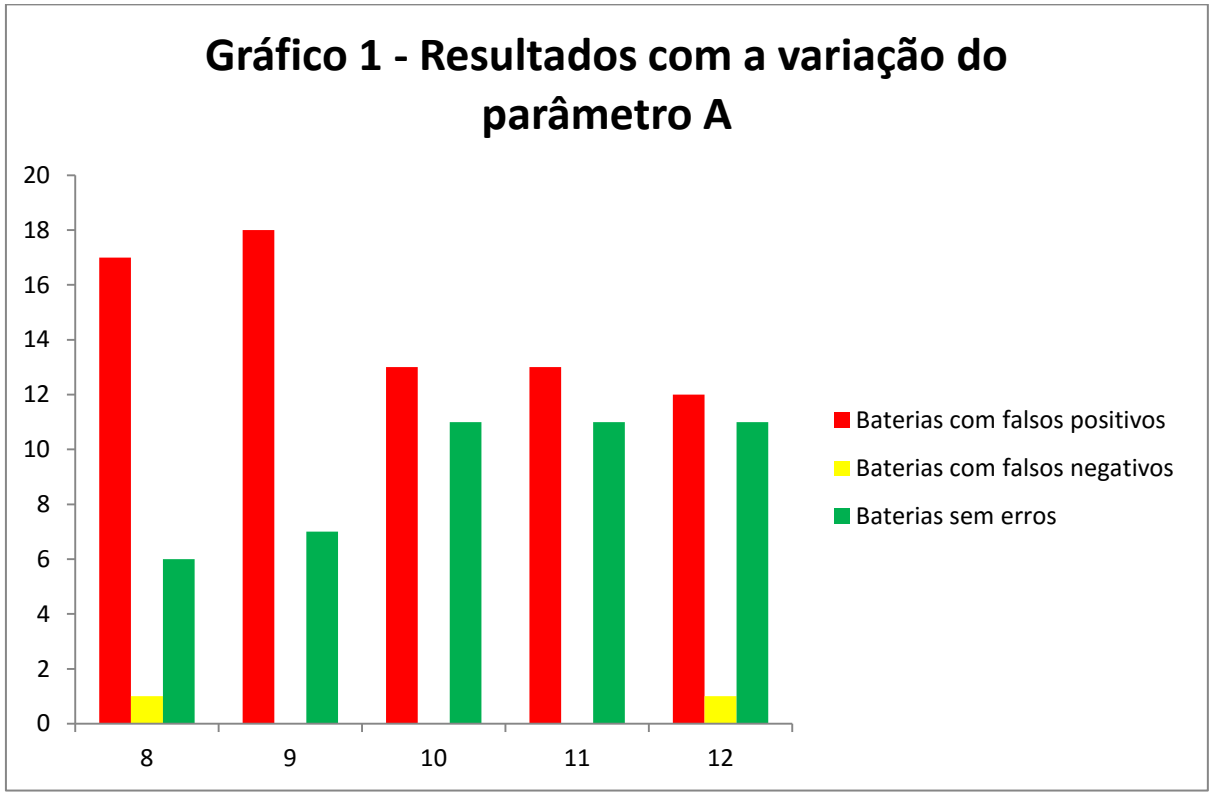
Tabela I.3: Teste 3	
Parâmetro	Valor
Alteração (A)	15
Alteração esperada (Ae)	70%
Bloco da Assinatura (B)	2
Bloco do Dither Reverso (Bdr)	2
Bloco de Verificação (Bv)	2
Rotação (R)	0
Taxa de aceitação (Ta)	80%
Falsos Positivos	0º
Falsos Negativos	3

Tabela I.4: Teste 4	
Parâmetro	Valor
Alteração (A)	25
Alteração esperada (Ae)	70%
Bloco da Assinatura (B)	2
Bloco do Dither Reverso (Bdr)	1
Bloco de Verificação (Bv)	1
Rotação (R)	0º
Taxa de aceitação (Ta)	70%
Falsos Positivos	0
Falsos Negativos	4

Tabela I.5: Teste 5	
Parâmetro	Valor
Alteração (A)	30
Alteração esperada (Ae)	70%
Bloco da Assinatura (B)	3
Bloco do Dither Reverso (Bdr)	3
Bloco de Verificação (Bv)	1
Rotação (R)	1º
Taxa de aceitação (Ta)	70%
Falsos Positivos	0
Falsos Negativos	0

Tabela I.6: Teste 6	
Parâmetro	Valor
Alteração (A)	30
Alteração esperada (Ae)	70%
Bloco da Assinatura (B)	3
Bloco do Dither Reverso (Bdr)	3
Bloco de Verificação (Bv)	1
Rotação (R)	5º
Taxa de aceitação (Ta)	70%
Falsos Positivos	0
Falsos Negativos	0

Apêndice II: Gráficos dos testes com cheque real



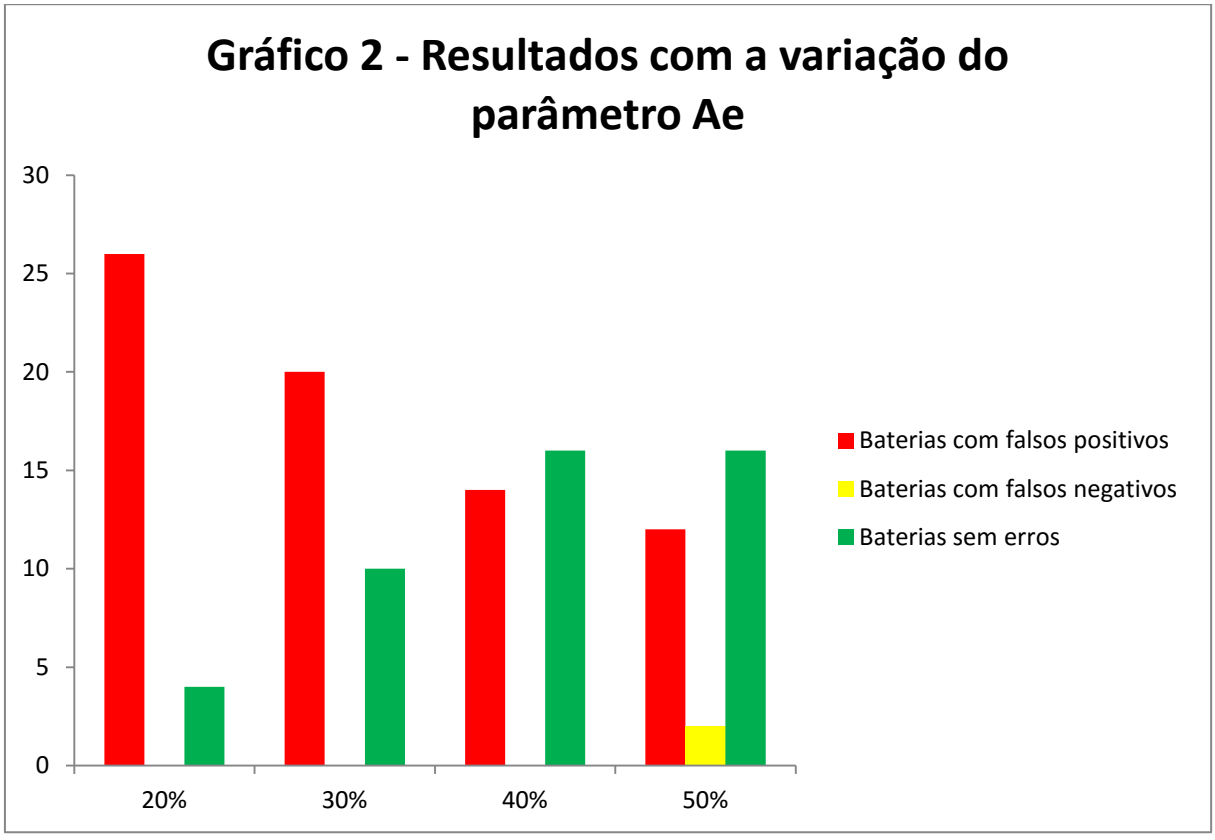



Gráfico 3 - Resultados com a variação do parâmetro B
40
35
30
25
20
15
10
5
0
2
3
Baterias com falsos positivos
Baterias com falsos negativos
Baterias sem erros

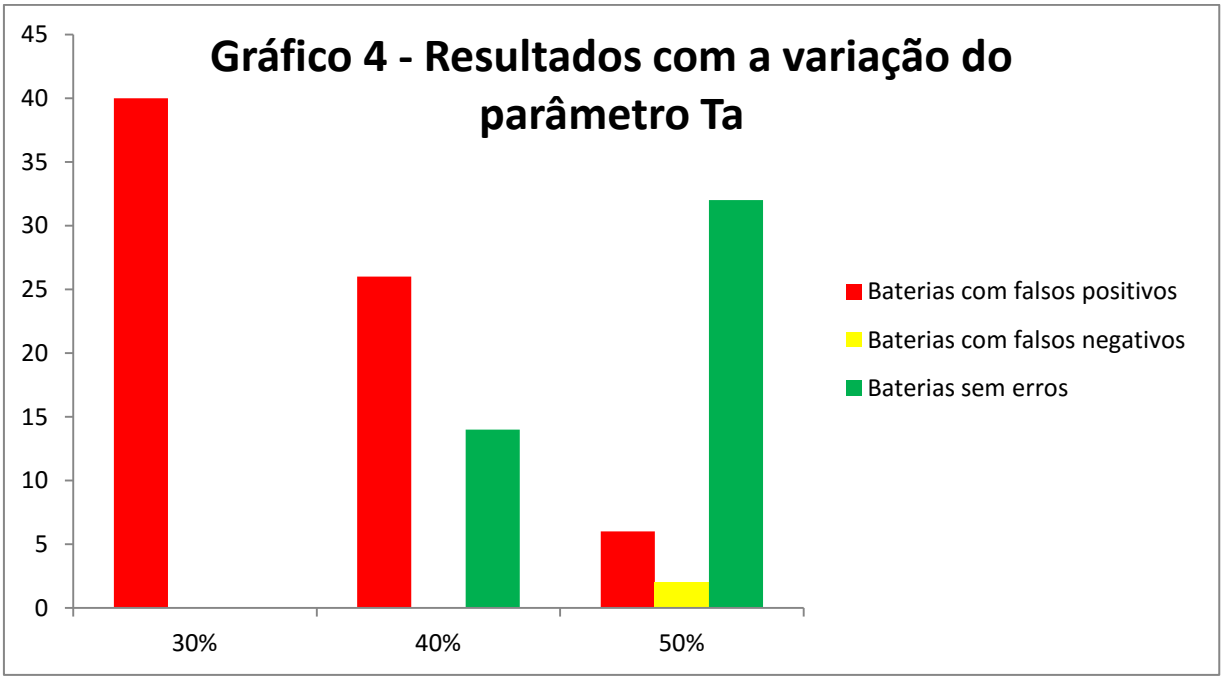


Gráfico 4 - Resultados com a variação do parâmetro Ta
45
40
35
30
25
20
15
10
5
0
30%
40%
50%
Baterias com falsos positivos
Baterias com falsos negativos
Baterias sem erros

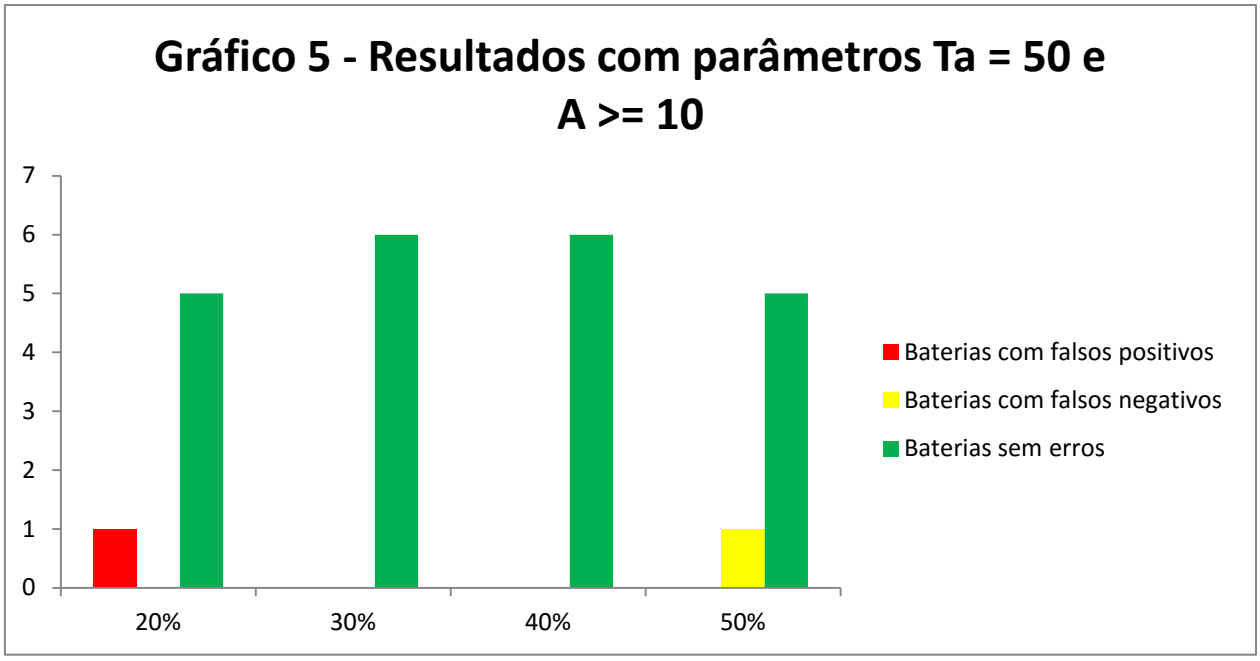


Gráfico 5 - Resultados com parâmetros Ta = 50 e A >= 10
7
6
5
4
3
2
1
0
20%
30%
40%
50%
Baterias com falsos positivos
Baterias com falsos negativos
Baterias sem erros